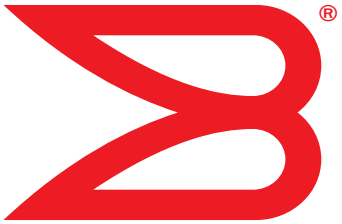
53-1002154-01
29 April 2011



FICON

Administrator's Guide

Supporting Fabric OS v7.0.0

BROCADE

Copyright © 2009-2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCFM, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, TurboIron, and Wingspan are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, Extraordinary Networks, MyBrocade, VCS, and VDX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
FICON Administrator's Guide	*53-1001348-01*	New document	July 2009
FICON Administrator's Guide	*53-1001771-01*	Updated document to include new features used with FICON.	March 2010
FICON Administrator's Guide	*53-1002154-01*	Updated document for Fabric OS version 7.0.0.	April 2011

Contents

About This Document

In this chapter vii
How this document is organized vii
Supported hardware and software viii
What's new in this document viii
Document conventions ix
- Text formatting ix
- Command syntax conventions ix
- Command examples x
- Notes, cautions, and warnings x
- Key terms x

Notice to the reader xi
Additional information xi
- Brocade resources xi
- Other industry resources xi

Getting technical help xii
Document feedback xiii

Chapter 1 Introducing FICON

In this chapter 1
FICON overview 1
- Fabric OS support for FICON 1
- Platforms supporting FICON 3
- Latency guideline 3
- Packet loss guideline 3
- Storage application guideline 3

FICON concepts 4
FICON configurations 6
- Switched point-to-point 6
- Cascaded FICON 7

Access control in FICON 8
- Cascaded zoning 9
- Error reporting 11
- Secure access control 11

FICON commands 13

Chapter 2 Administering FICON Fabrics

In this chapter 15
User security considerations 15
Meeting Query Security Attribute requirements 15
Preparing a switch for FICON 17
Cascaded FICON and 2-byte addressing considerations 17
Configuring switched point-to-point FICON 18
Configuring cascaded FICON 21
FICON and FICON CUP in Virtual Fabrics 22
Flat addressing mode 22
256-area addressing mode 22
Changing the addressing mode 23
Moving ports to a logical switch 24
Clearing the FICON management database 24

Chapter 3 Configuring FICON CUP

In this chapter 27
Control Unit Port overview 27
FICON CUP restrictions 29
CUP configuration recommendations 29
FICON CUP zoning and PDCM considerations 30
Port and switch naming standards for FMS 30
FICON CUP Fabric OS commands 30
Configuring FICON CUP 31
Configuring FICON CUP in Virtual Fabrics 32
Determining physical port assignment 33
FMS mode and FICON CUP 34
Displaying FMS mode 35
Enabling FMS mode 35
Disabling FMS mode 35
Setting up FICON CUP if FMS mode is enabled 35
FMS mode and FICON OxFE or OxFF addresses 36
Upgrade considerations 36
Mode register bit settings 37
FICON file access facility 38
Setting the mode register bits 39
Setting the MIHPTO value 40
Persistently enabling and disabling ports for CUP 40

Chapter 4 Administering FICON Extension Services

In this chapter 43

FICON emulation overview 43
IBM z/OS Global Mirror emulation 44
Tape emulation 45
Teradata emulation 47
Platforms supporting FICON extension over IP 48
FCIP configuration requirements for FICON extension 48
Configuration requirements for switches and directors 48
High integrity fabric requirements for cascaded configurations 48
FICON emulation requirement for a determinate path 48
Configuring FICON emulation 50
Configuring emulation on the FR4-18i blade 51
Configuring emulation on the 7800 switch and FX8-24 blade 51
Displaying FICON emulation configuration values 51
Modifying FICON emulation 53
Displaying FICON emulation performance statistics 53
FICON emulation monitoring 53
FICON emulation statistics 55

Chapter 5 Maintaining and Troubleshooting FICON

In this chapter 61
Firmware management in a FICON environment 61
Upgrade and downgrade considerations 61
Firmware upgrade disruption 62
Non-disruptive firmware upload and download 62
Configuration restoration in a FICON environment 62
Traffic Isolation Zoning 63
Determining ports for the TI Zone 63
Enhanced TI Zoning 64
Port fencing 70
Defining port fencing 70
Settings for FICON environments 70
FICON information 71
Link incidents 71
Registered listeners 72
Node identification data 72
FRU error reporting 72
Port swapping 74
Blade swapping 75
Common FICON issues 76

Troubleshooting FICON 79
General information to gather for all cases 79
Switched point-to-point topology checklist. 80
Cascaded topology checklist. 80
Gathering additional information 81
Troubleshooting FICON CUP 81
Troubleshooting NPIV 82

Appendix A **Configuration Information Record**

Appendix B **EBCDIC Code Page**

Index

About This Document

In this chapter

- How this document is organized vii
- Supported hardware and software. viii
- What's new in this document viii
- Document conventions ix
- Notice to the reader xi
- Additional information xi
- Getting technical help xii
- Document feedback xiii

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, "Introducing FICON" provides basic FICON concepts.
- Chapter 2, "Administering FICON Fabrics" allows you to set up and get started using FICON quickly, if you are already familiar with FICON concepts and basic procedures.
- Chapter 3, "Configuring FICON CUP" provides basic conceptual information on FICON CUP and instructions on how to set CUP up in your FICON environment.
- Chapter 4, "Administering FICON Extension Services" provides basic conceptual information on emulation products and how to set them up in a FICON environment.
- Chapter 5, "Maintaining and Troubleshooting FICON" discusses maintaining your switch in a FICON environment, provides symptoms, troubleshooting tips, and possible solutions to known issues.
- Appendix A, "Configuration Information Record" provides a form to record your FICON configuration information.
- Appendix B, "EBCDIC Code Page" provides a table of the EBCDIC Code Page 37.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Fabric OS v7.0, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of *Fabric OS v7.0:*

- Brocade 5100 switch
- Brocade 5300 switch
- Brocade 6510 switch
- Brocade 7800 Extension Switch
- FR4-18i Extension Blade
- FX8-24 Extension Blade
- Brocade DCX Backbone
- Brocade DCX-4S Backbone

What's new in this document

- Information that was added:
  - "Moving ports to a logical switch" on page 24
  - "FMS mode and FICON OxFE or OxFF addresses" on page 36
  - "Upgrade considerations" on page 36
  - "FICON and ESCON conversion support" on page 47
  - "Teradata emulation" on page 47
  - "FICON emulation statistics" on page 55
  - "FRU error reporting" on page 72
- Information that was changed:
  - "FICON emulation overview" on page 43. Added detailed licensing information for features.
  - "Tape Write Pipelining" on page 46. Added details on feature function.
  - "Configuring emulation on the 7800 switch and FX8-24 blade" on page 51. Added Teradata emulation options.
  - "Displaying FICON emulation configuration values" on page 51. Added display for Teradata emulation.
  - "Port swapping" on page 74. Added note that you cannot swap ports with area OxFE or OxFF addresses with FMS enabled.
  - "Blade swapping" on page 75. Added note that you cannot swap blades with area OxFE or OxFF addresses with FMS enabled.

- Information that was deleted:
  - “Cross-coupled configurations” section in Chapter 4.
  - Information on interopmode and M-Series switches. FICON M-Series connections, interopmode, McDATA fabric mode, and McDATA open fabric mode are no longer supported.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
code text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	**Commands are printed in bold.**
--**option, option**	Command options are printed in bold.
-**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, --**show** WWN
|	Boolean. Elements are exclusive. Example: --**show** -**mode** egress | ingress

Command examples

This guide describes how to perform configuration tasks using the Fabric OS command line interface, but does not describe the commands in detail. For complete descriptions of all Fabric OS commands, including syntax, operand descriptions, and sample output, see the *Fabric OS Command Reference*.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on MyBrocade. See "Brocade resources," for instructions on accessing MyBrocade.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
International Business Machines Corp.	IBM, FICON, S/390, z/OS, zSeries, Series z, Redbooks, z/OS Global Mirror
Teradata Corporation	Teradata
Optica Technologies, Inc.	Prizm FICON to ESCON converter and ESBT Bus/Tag Interface Module for Prizm

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, go to *http://my.brocade.com* and register at no cost for a user ID and password.

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

http://www.brocade.com

Release notes are available on the MyBrocade website and are also bundled with the Fabric OS firmware.

Other industry resources

- White papers, online demonstrations, and data sheets are available through the Brocade website at *http://www.brocade.com/products/software.jhtml*.
- Best practice guides, white papers, data sheets, and other documentation is available through the Brocade Partner website.

For additional resource information, visit the Technical Committee T11 website. This website provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association website:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information
    - Switch model
    - Switch operating system version
    - Error numbers and messages received
    - **supportSave** command output
    - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
    - Description of any troubleshooting steps already performed and the results
    - Serial console and Telnet session logs
    - syslog message logs
2. Switch Serial Number

    The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below:

    The serial number label is located as follows:

    - *Brocade 300, 5100, 5300, 7800, 8000, VA-40FC,* 6510, and *Brocade Encryption Switch*—On the switch ID pull-out tab located inside the chassis on the port side on the left
    - Brocade 5410, M5424, 5450, 5460, 5470, 5480—Serial number label attached to the module
    - *Brocade DCX*—On the bottom right on the port side of the chassis
    - *Brocade DCX-4S*—On the bottom right on the port side of the chassis, directly above the cable management comb
3. World Wide Name (WWN)

    Use the **licenseIDShow** command to display the switch WWN.

    If you cannot use the **licenseIDShow** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1

Introducing FICON

In this chapter

- FICON overview 1
- FICON concepts 4
- FICON configurations 6
- Access control in FICON 8
- FICON commands 13

FICON overview

IBM Fibre Connection (FICON®) is an industry-standard, high-speed input/output (I/O) interface for mainframe connections to storage devices. This guide discusses support offered by Fabric OS in intermix mode operations, in which FICON and Fibre Channel technology work together.

For specific information about intermix mode and other aspects of FICON, refer to the IBM Redbook, *FICON® Implementation Guide* (SG24-6497-01), and *Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches* (SG24-6116-08).

NOTE
In this guide, the term *switch* is used to refer to a Brocade switch, director, or backbone platform unless otherwise noted.

Fabric OS support for FICON

The following Fabric OS standard features support FICON fabrics:

- Blade swapping

  Allows you to swap a blade of the same type so that you can perform a FRU replacement with minimal traffic disruption. This feature is available for both FICON and open system environments. Blade swapping resolves situations in which the hardware has failed and the channel configurations cannot be changed quickly. Blade swapping has minimal or no impact on other switch features.

- Device connection control (DCC) policy

  Used to restrict which Fibre Channel device ports can connect to which Fibre Channel switch ports.

- FICON MIB module

  Addresses link incident data for FICON hosts and devices connected to a switch. It supplements other MIBs used to manage switches and should be used in conjunction with those other MIBs. For more information, Refer to the *Fabric OS MIB Reference*.

- Insistent domain ID (IDID)

  Allows the switch to insist on a specific domain ID before joining a fabric. This feature guarantees that a switch operates only with its preassigned domain ID.

- Link incident detection, registration, and reporting

  Provides administrative and diagnostic information.

- Port swapping

  Redirects resources from a failed port to a healthy port without changing the mainframe hardware configuration definition (HCD) settings. Port swapping is available for both FICON and open system environments. Port swapping resolves situations in which the hardware has failed and the channel configurations cannot be changed quickly. Port swapping has minimal or no impact on other switch features.

- Switch connection control (SCC) policy

  Includes switch binding security methods that prevent unauthorized switches from joining a fabric.

- Traffic Isolation (TI) Zones and Enhanced TI Zones

  TI Zones are used to direct traffic across links through a specified path. Enhanced TI Zones allow you to have ports in more than one TI Zone and to program domain controller routes to destination domains for F-class traffic, ensuring fabric stability.

Brocade management tools provide further support:

- Brocade Network Advisor (BNA)

  Brocade Network Advisor is an optional software program that can be used to manage a fabric that supports FICON and FCP devices and traffic. This is the recommended GUI management tool for FICON environments on B-series enterprise-class switches. For more information on Brocade Network Advisor refer to the manual appropriate for your version requirements:

  - *Brocade Network Advisor SAN + IP User Manual*
  - *Brocade Network Advisor SAN User Manual*

- *Fabric OS MIB Reference*

  The MIB reference provides information and procedures on setting up the SNMP agent and FICON Management Information Base (MIB) on your switch.

- Web Tools

  Web Tools is an embedded GUI management tool that can be used to manage a director (switch) that supports FICON and Fibre Channel Protocol (FCP) devices and traffic. For more information on Web Tools, refer to the *Web Tools Administrator's Guide*.

NOTE
Some licenses are installed and activated on the switch at the factory. Use a Brocade management interface to verify that the required licenses are installed and activated on the switch.

Platforms supporting FICON

FICON protocol is supported on the following Brocade models for this release:

- Brocade DCX and DCX-4S Backbones (FC8-16 and FC8-32 port blades), FR4-18i and FX8-24 FCIP blades, and the FC10-6 10 Gbps port blade for ISL connections. The DCX, the FC8-48 blade is only supported in a logical switch defined for zero-based addressing.
- Brocade 5100 and 5300 switches.
- Brocade 6510 switch.
- The Brocade 7800 Extension Switch and the Brocade FR4-18i (for the Brocade DCX and DCX-4S) and FX8-24 blade (for the Brocade DCX and DCX-4S) provide FICON over IP extension.

The following port blades are not supported in a FICON environment unless otherwise noted:

- FCOE10-24
- FS8-18
- FC4-48
- In the DCX, the FC8-48 blade is only supported in a logical switch defined for zero-based addressing.
- FC8-64

In an Admin Domain-enabled fabric, you should put all of the ports on the FC8-48 and FC8-64 blades in an Admin Domain other than the one used for FICON ports. The ports on these blades should not belong to the zone in which FICON devices are present.

In all switches and directors that have FICON devices attached, or where FICON traffic will be carried, the port-based routing policy is required (**set aptPolicy option 1**). Exchange based routing (**set aptPolicy option 3**) is only supported when Lossless is specified. It is recommended that you enable Lossless, regardless of the routing policy.

Latency guideline

The maximum allowable network round trip latency is typically 200 ms. This is application, dependent, and for some applications it may be lower. For synchronous mirroring applications, the maximum latency is typically less than 10 ms. These values are to maintain data throughput performance. However, many synchronous applications can run in asynchronous mode, allowing more than one outstanding I/O per transaction.

Packet loss guideline

The end-to-end network should maintain less than 1 percent packet loss for optimum performance. Performance degradation is exponential as packet loss increases above 1 percent. It is highly recommended that you obtain an Service Level Agreement (SLA) with your network provider that reflects this requirement.

Storage application guideline

Storage applications will operate more efficiently if they are tuned to match the outstanding amount of data to the characteristics of the IP connection, such that there is always data being transmitted. Generally speaking, with higher latency and higher bandwidth, more data can exist in the WAN network.

FICON concepts

Figure 1 shows how the traffic in a switched point-to-point configuration flows in a FICON environment. The logical path of the traffic is defined as frames moving from the channel to the switch to the control unit. FICON traffic moves from a logical partition (LPR) and through the channel, through a Fibre Channel link to the switch through the control unit, and ending at the device. This is also called a *channel path*, which is a single interface between a central processor and one or more control units along which signals and data can be sent to perform I/O requests. The channel path uses the logical path to traverse the Fibre Channel fabric. The channel path is defined using an ID, called the channel path ID (CHPID). This information is stored in the Input/Output Configuration Program (IOCP) so that the same path is used. The IOCP is a z/OS program that defines to a system the channels, I/O devices, paths to the I/O devices, and the addresses of the I/O devices. The output is normally written to a z/OS or zSeries Input/Output Configuration Data Set (IOCDS). The data set in the z/OS and zSeries processor (in the support element) contains an I/O configuration definition built by the IOCP Work Load Manager.

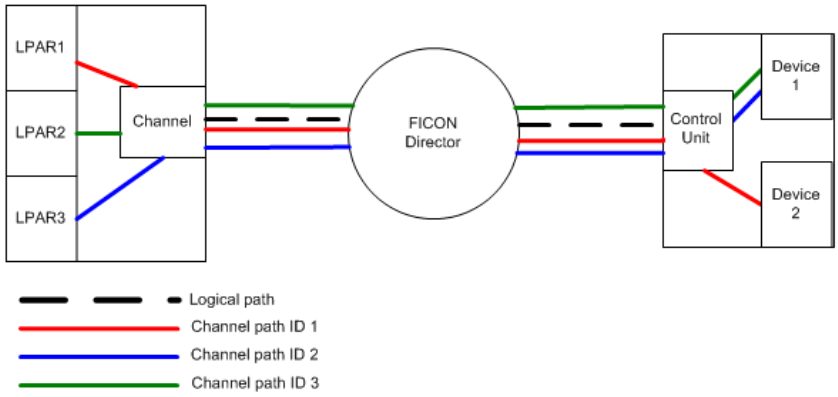


FIGURE 1 FICON traffic

The traffic on the channel path communicates using channel command words (CCWs) that direct the device to perform device specific actions, such as Seek, Read, or Rewind. In a FICON environment, CCWs use the buffer credit process for information unit (IU) pacing. IU pacing is a mechanism that limits the number of CCWs, and therefore the number of IUs, that can either transmit (write) or solicit (read) without the need for additional control-unit-generated acknowledgements called *command responses*. There are times when there are no more buffer credits to pass back to the other end and a frame pacing delay occurs. Frame pacing delay is the number of intervals of 2.5 microsecond duration that a frame had to wait to be transmitted due to a lack of available buffer credits.

FICON introduces the following concepts:

- FICON Control Unit Port (CUP)

  The internal port in a switch that assumes an FC address such that it is the FC DID used to direct FICON traffic to the FICON Management Server.

- FICON Manager

  Host communication includes control functions such as blocking and unblocking ports, as well as monitoring and error-reporting functions.

- Hardware Configuration Definition (HCD)

  HCD is an IBM interactive interface application that allows you to define the hardware configuration for both the processor channel subsystem and the operating system running on the processor.

- Information unit

  A unit of FICON data consisting of from one to four Fibre Channel frames.

- Link Incident Record Registration (LIRR)

  The LIRR Extended Link Service (ELS) requests that the recipient add the requesting port to its list of ports that are to receive a Registered Link Incident Report (RLIR).

- Node

  A node is an endpoint that contains information. It can be a computer (host), a device controller, or a peripheral device, such as a disk array or tape drive. A node has a unique 64-bit identifier known as the Node_Name. The Node_Name is typically used for management purposes.

- Prohibit Dynamic Connectivity Mask (PDCM) and connectivity attributes

  PDCM controls whether or not communication between a pair of ports in the switch is prohibited. Connectivity attributes control whether all the communication is blocked for a port.

- Read Record Set (RRS)

  RRS is an IBM Channel-initiated CCW command. The Brocade's FCIP FICON Acceleration License allows the emulation of command chains that include this CCW command. The command is used in IBM z/OS Global Mirror configurations to read updates from a volume in an active mirroring session.

- Registered Link Incident Report (RLIR)

  RLIR ELS provides a way for a node port to send an incident record to another node port.

- Request Node Identification Data (RNID)

  RNID ELS acquires the associated node’s identification data, which provides configuration discovery and management purpose information.

- Resource Measurement Facility (RMF)

  A monitoring function that gathers transaction data from the environment and generates performance reports. All Level II reports, which include port statistics, require CUP and FMS. Keep RMF active in the system 24 hours a day, and run it at a dispatching priority above that of other address spaces in the system. If you do, reports are written at the requested intervals and other work is not delayed because of locks held by RMF.

- Systems Operations (SysOps)

  SysOps provides the ability to monitor and control all subsystems in a sysplex from any system in the sysplex. This includes controlled startup, controlled shutdown, and automated recovery of software resources.

- Sysplex

  In IBM mainframe computers, a Systems Complex, commonly called a *sysplex*, allows multiple processors to be joined into a single unit, sharing the same sysplex name and Couple Data Sets.

FICON configurations

There are two types of FICON configurations that are supported using Brocade Fabric OS: switched point-to-point and cascaded topologies.

Switched point-to-point

A single-switch configuration is called *switched point-to-point* and requires that the channel is configured to use single-byte addressing. If the channel is set up for 2-byte addressing, then the cascaded configuration setup applies. Figure 2 illustrates an example of the switched point-to-point configuration.

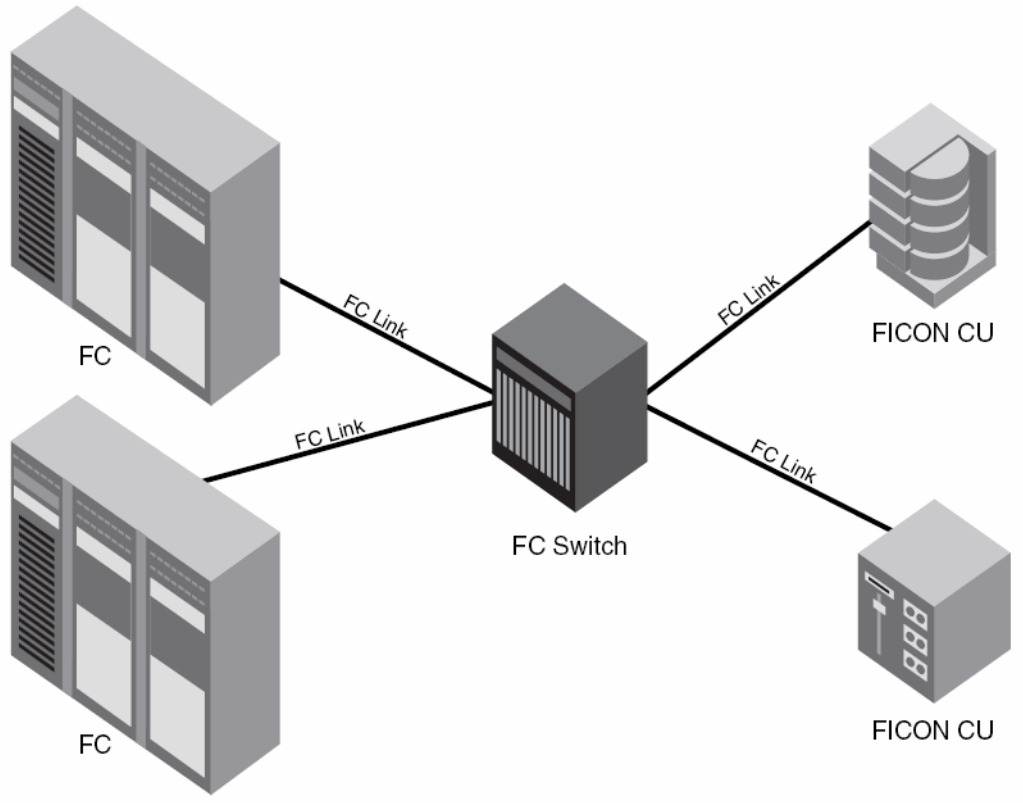


FIGURE 2 Switched point-to-point FICON

Cascaded FICON

Cascaded FICON refers to an implementation of FICON that involves one or more FICON channel paths defined over two FICON switches connected to each other using an Inter-Switch Link (ISL). The processor interface is connected to one switch, while the storage interface is connected to the other. This configuration is supported for both disk and tape, with multiple processors, disk subsystems, and tape subsystems sharing the ISLs between the directors. Multiple ISLs between the directors are also supported. Cascading between a director and a switch, from a Brocade DCX enterprise-class platform to a Brocade 5100 for example, is also supported.

A cascaded configuration (Figure 3) requires a list of authorized switches. This authorization feature, called *fabric binding,* is available through the Secure Access Control List feature. The fabric binding policy allows a predefined list of switches (domains) to exist in the fabric and prevents other switches from joining the fabric. This type of configuration is described in "User security considerations" on page 15.

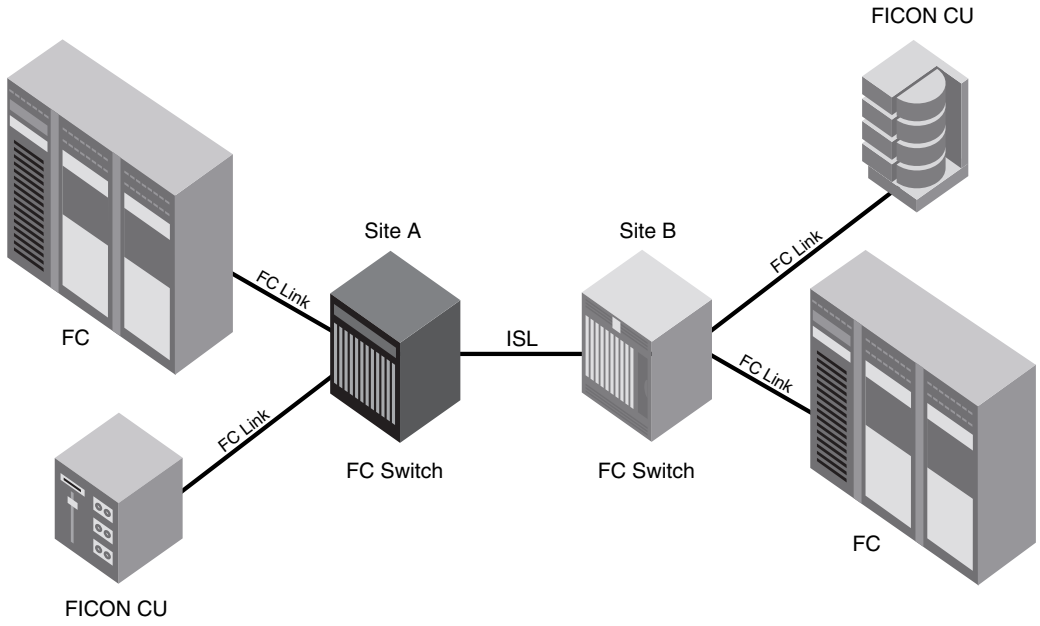


FIGURE 3 Cascaded FICON

There are hardware and software requirements specific to cascaded FICON:

- The FICON directors themselves must be from the same vendor (that is, both should be from Brocade).
- The mainframes must be zSeries machines or System z processors: z196, z800, 890, 900, 990, z9 BC, z9 EC, z10 BC and EC. Cascaded FICON requires 64-bit architecture to support the 2-byte addressing scheme. Cascaded FICON is not supported on 9672 G5/G6 mainframes.
- z/OS version 1.4 or later, or z/OS version 1.3 with required PTFs/MCLs to support 2-byte link addressing (DRV3g and MCL (J11206) or later) is required.
- The high integrity fabric feature for the FICON switch must be installed on all switches involved in the cascaded architecture.

Figure 4 and Figure 5 show two cascaded configurations. These configurations require Channel A to be configured for 2-byte addressing and require IDID and fabric binding. It is recommended that there be only two domains in a path from a FICON Channel interface to a FICON Control Unit interface. There are exceptions to the two-domain rule when extended fabric solutions are deployed.

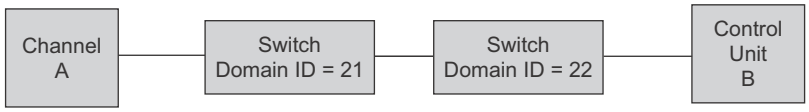


FIGURE 4 Cascaded configuration, two switches

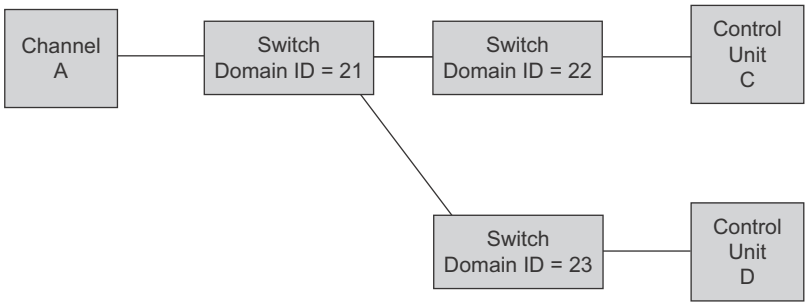


FIGURE 5 Cascaded configuration, three switches

Access control in FICON

Zoning is used to control access in a FICON environment. A zone consists of a group of ports or WWNs. Connectivity is permitted only between connections to the switch that are in the same zone. There are three types of zoning: WWN, port, and domain,index zoning. A zone configuration includes at least one zone. In open systems environments and in more complex FICON deployments, the zone configuration contains multiple zones. Although domain,index zoning is supported, WWN zoning for QoS is recommended in environments where NPIV is deployed. For more information on how to implement QoS domain index zoning in your fabric, refer to the *Fabric OS Administrator's Guide*.

When zoning changes occur, Registered State Change Notification (RSCN) messages are sent out throughout the zone. RSCNs are part of the low-level Fibre Channel protocol that alerts channels and devices to changes in the fabric. Using multiple smaller zones instead of one large zone helps alleviate the need for channels and device interfaces to process RSCNs that are not relevant.

Cascaded zoning

Figure 6 illustrates multiple sites sharing the same disaster recovery site. Each director at a remote site—labeled Director 1 and Director 3—can pass traffic to Director 2, but no traffic is permitted between Zone A and Zone B.

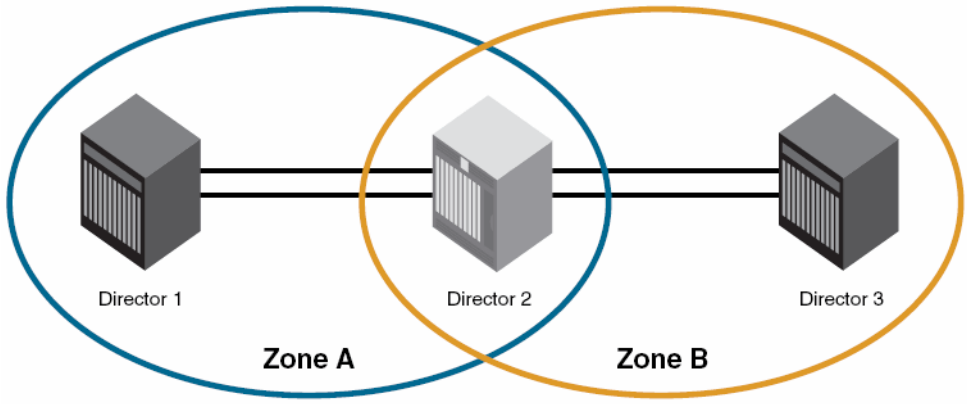


FIGURE 6 Simple cascaded zoning

Figure 7 illustrates the multiple zoning concepts that can be used to restrict traffic. In Figure 7, any host channel at the Backup Site (connected to Director 11 or Director 12) can connect to the backup tape contained within the same zone. Notice that no more than a single hop is ever allowed and only Channel Path Identifiers (CHPIDs) 79 and 7A on the Primary Site can connect to the backup tape. Furthermore, CHPIDs 79 and 7A can only connect to the backup tape at the Backup Site.

NOTE
Zoning does not replace the need to set up the connectivity from the host to storage control units in the HCD or IOCP.

For more information on zoning, refer to the *Fabric OS Administrator's Guide*.

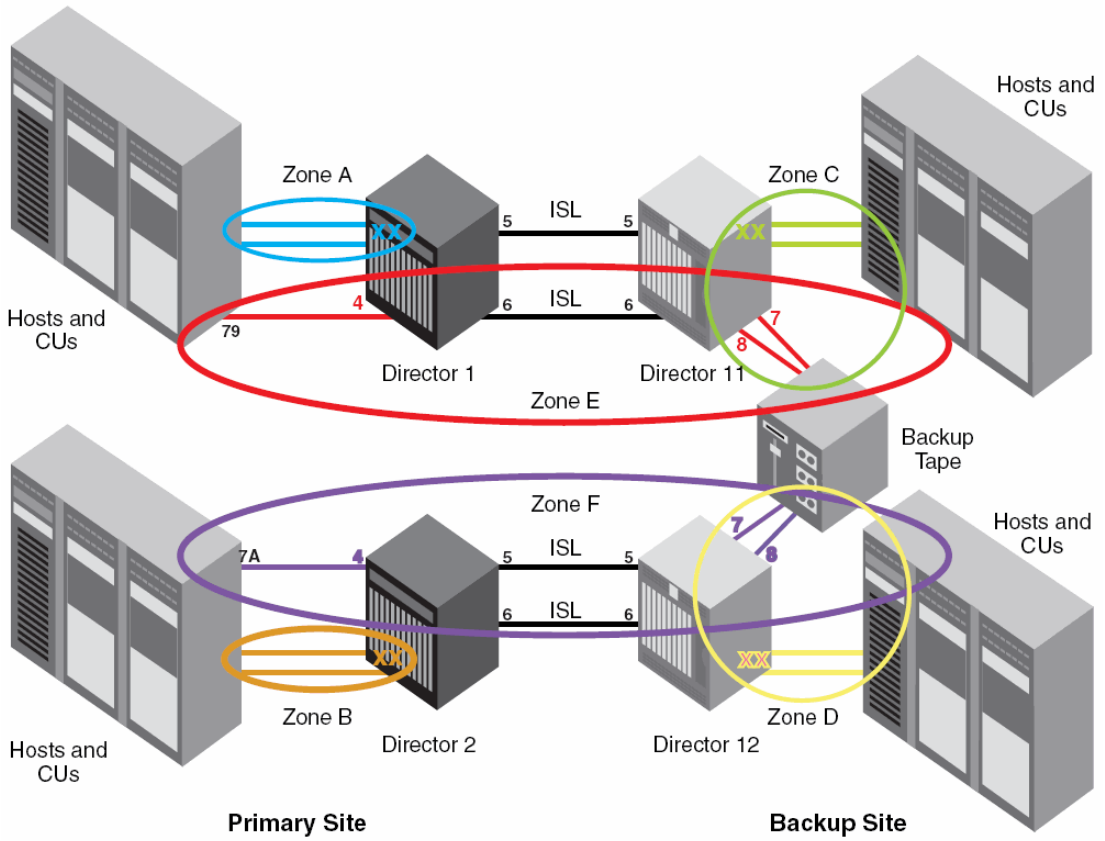


FIGURE 7 Complex cascaded zoning

Blue Zone A: Any CHPID connected to Director 1, except CHPID 79, can get to any control unit connected to Director 1. The zone includes all ports in Director 1 except ports 4, 5, and 6.

Orange Zone B: Any CHPID connected to Director 2, except CHPID 7A, can get to any control unit connected to Director 2. The zone includes all ports in Director 2 except ports 4, 5, and 6.

Green Zone C: Any CHPID connected to Director 11 can get to any control unit connected to Director 11. The zone includes all ports in Director 11 except ports 5 and 6. Adding ports 5 and 6 to the zone, so that all ports in the director are in the same zone, would not affect permitted connectivity and may be a more practical alternative.

Yellow Zone D: Any CHPID connected to Director 12 can get to any control unit connected to Director 12. The zone includes all ports in Director 12 except ports 5 and 6, which are used for ISLs.

Red Zone E: CHPID 79 can talk only to the remote tape connected to ports 7 and 8 on Director 11. The zone includes port 4 of Director 1 and ports 7 and 8 of Director 11. Either ISL can be used.

Purple Zone F: CHPID 7A can talk only to the remote tape connected to ports 7 and 8 on Director 12. The zone includes port 4 of Director 2 and ports 7 and 8 of Director 12. Either ISL can be used.

Error reporting

Non-implicit (such as Network Operating System (NOS) recognized or bit error rate threshold exceeded) and implicit (FRU failure) link incidents are reported to registered listeners on the local switch. The RMF 74-7 record (FICON Director Activity Report, which is the same RMF Record containing the average frame pacing delay information) reports port errors, which in turn are also reported back to the mainframe host management consoles.

Secure access control

Binding is a method used to prevent devices from attaching to the switch. Secure Access Control List (ACL) provides the following fabric, switch, and port binding features:

- *Fabric binding* is a security method for restricting switches within a multiple-switch fabric. Use an SCC policy to prevent unauthorized switches from joining a fabric.
- *Switch binding* is a security method for restricting devices that connect to a particular switch. If the device is another switch, this is handled by the SCC policy. If the device is a host or storage device, the device connection control (DCC) policy binds those devices to a particular switch. Policies range from completely restrictive to reasonably flexible, based upon customer needs.
- SCC ACL with strict fabric-wide consistency is necessary for FICON switch binding.
- *Port binding* is a security method for restricting host or storage devices that connect to particular switch ports. The DCC policy also binds device ports to switch ports. Policies range from completely restrictive to reasonably flexible, based on customer needs.

  Figure 8 on page 12 demonstrates the three types of binding you can use depending on the security requirements of your fabric.

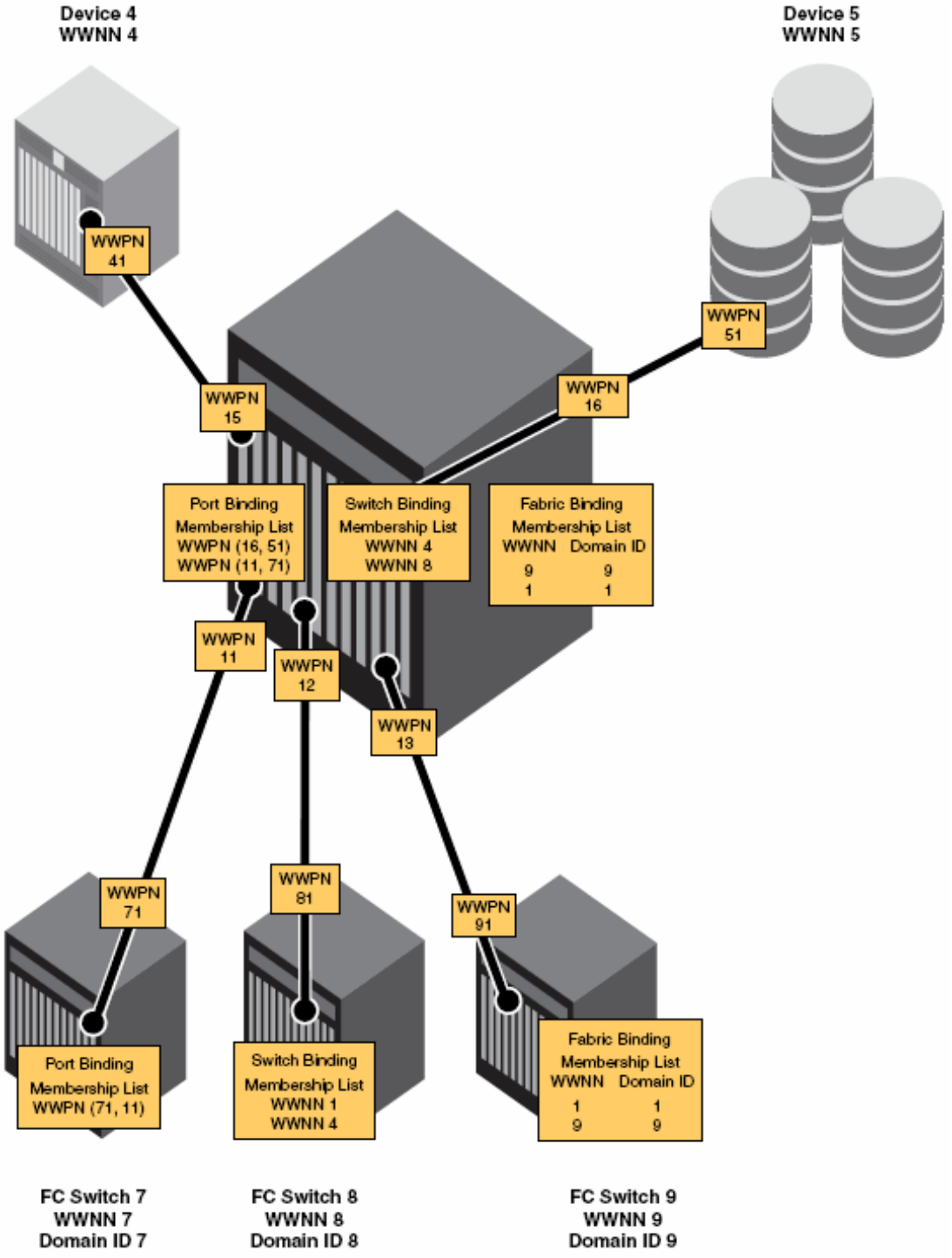


FIGURE 8 Three types of binding

FICON commands

NOTE
The Fabric OS CLI supports only a subset of the Brocade management features for FICON fabrics. The full set of FICON CUP administrative procedures is available using the Brocade Network Advisor and Web Tools software features. You can also use an SNMP agent and the FICON Management Information Base (MIB).

Table 1 summarizes the Fabric OS CLI commands that can be used for managing FICON fabrics. For detailed information on these commands, see the *Fabric OS Command Reference*.

TABLE 1 Fabric OS commands related to FICON

Command	Description
Standard Fabric OS commands	
bladeSwap	Swaps the area numbers for matching port pairs of two blades.
configure	Changes a variety of switch configuration settings, including setting the domain ID and the insistent domain ID mode.
configUpload	Backs up the current configuration.
firmwareShow	Displays the current version of the firmware.
licenseAdd	Adds a license to the switch. The license key is case-sensitive and must be entered exactly.
licenseRemove	Removes a license from the switch. Note that FMS mode must be disabled before removing the FICON license.
licenseShow	Displays current license keys, along with a list of licensed products enabled by these keys.
licenseSlotCfg –add	Enables slot-based licenses for a switch chassis. Note that for a switch without blades, such as the 7800 Extension Switch, slot 0 is used as the slot-based license target. For blades, slot numbers are based on the switch chassis numbering scheme. A license key with the specified capacity must be installed with the **licenseAdd** command before you can enable a feature on a specified slot with this command.
licenseSlotCfg –show	Displays all slot-based licenses in the chassis.
portAddress –bind	Binds the 16-bit address to the lower two bytes of a port 24-bit Fibre Channel address.
portAddress –unbind	Unbinds the currently bound address for the specified port.
portSwap	Swaps ports.
portSwapDisable	Disables the **portSwap** command.
portSwapEnable	Enables the **portSwap** command.
portSwapShow	Displays information about swapped ports.
supportShowCfgEnable ficon	Turns on logging of FICON information on the switch.
Commands specific to FICON	
ficonclear rlir	Removes all RLIR records from the local RLIR database.
ficonclear rnid	Removes all outdated RNID records from the local RNID database.

TABLE 1 Fabric OS commands related to FICON (Continued)

Command	Description
ficoncfg --set LIRR <*portnumber*>	Sets the current LIRR device port number persistently.
ficoncfg --reset LIRR <*portnumber*>	Clears the currently configured LIRR port number.
ficonhelp	Displays a list of FICON support commands.
ficonshow lirr [**fabric**]	Displays registered listeners for link incidents for the local switch or for the fabric, if specified.
ficonshow rlir [**fabric**]	Displays link incidents for the local switch or for the fabric, if specified.
ficonshow rnid [**fabric**]	Displays node identification data for all devices registered with the local switch or all devices registered with all switches defined in the fabric, if specified.
ficonshow switchrnid [**fabric**]	Displays node identification data for the local switch or for the fabric, if specified.

Chapter

2

Administering FICON Fabrics

In this chapter

- User security considerations 15
- Preparing a switch for FICON 17
- Configuring switched point-to-point FICON 18
- Configuring cascaded FICON 21
- FICON and FICON CUP in Virtual Fabrics 22
- Clearing the FICON management database 24

User security considerations

To administer FICON, you must have one of the following roles associated with your login name on the switch:

- Admin
- Operator
- SwitchAdmin
- FabricAdmin

The User and BasicSwitchAdmin roles are view-only. The ZoneAdmin and SecurityAdmin roles have no access.

In an Admin Domain-aware fabric, if you use the FICON commands (**ficonShow**, **ficonClear**, **ficonCupShow**, and **ficonCupSet**) for any Admin Domain other than AD0 and AD255, the current switch must be a member of that Admin Domain. The output is not filtered based on the Admin Domain.

Meeting Query Security Attribute requirements

In a cascaded switch configuration, FICON channels use a Query Security Attributes (ELS QSA) function to determine whether they are connected to a high integrity fabric. When a FICON channel is connected to a fabric that is not high integrity, the physical CHPID (PCHID) will go into an invalid attachment/isolated state (drop light), which then requires you to recover using the CPU Hardware Management Console (HMC).

To ensure the FICON Channel QSA requirements have been met, be sure to configure the following features:

- Insistent domain ID
- Fabric Wide Consistency Policy => SCC:S (Strict mode)

Enabling insistent domain ID

To enable Insistent Domain ID, follow these steps for each switch in the fabric:

1. Connect to the switch and log in using an account assigned to the admin role
2. Enter the configure command and step through the interactive prompts.
   a. At the “Fabric parameters” prompt, type y.
   b. At the “Insistent Domain ID Mode” prompt, type y.

Enabling the fabric-wide consistency policy

Enable the fabric wide consistency policy after all the switches have joined the merged fabric. If there are fdd conflicts on any of the ISLs, disable the fabric-wide consistency policy on each switch in the fabric.

Once the fabric has merged successfully (use **fabricshow** to verify) then enter the following command.

```
fddcfg --fabwideset "SCC:S"
```

Note that the :S enforces strict mode, which is required for FICON.

Using other security commands

Following are some other security-related commands that you might find useful.

Disabling fabric-wide consistency policy.

To disable the policy, enter the following command.

```
fddcfg --fabwideset ""
```

Displaying fabric-wide consistency policy

To display fabric-wide consistency policy information, enter the following command:

```
fddcfg --showall
```

Displaying the current Security Policy

To display the current security policy, enter the following command:

```
secpolicyshow
```

Creating SCC policy

To create the switch connection control (SCC) policy and define the WWN of switches allowed in the fabric, perform the following steps on each switch in the fabric. This adds all switches in the fabric, if they are connected.

1. Enter the following command to create the SCC policy.

   ```
   secpolicycreate "SCC_POLICY","*"
   ```

   You can also use the following command.

   ```
   secpolicyadd "SCC_POLICY","wwn1;wwn2"
   ```

2. Enter the following command.

```
secpolicyactivate
```

Deleting SCC_POLICY

Enter the following command if you get messages that the E_Port in a security violation state.

```
secpolicydelete "SCC_POLICY"
```

Recovering the E_Port

Enter the following commands for each switch if the E_Port is down.

```
secpolicyactivate
portenable n
```

Preparing a switch for FICON

The following steps are provided for you to verify and prepare a switch for use in a switched point-to-point FICON environment. Single-switch configuration does not require insistent domain IDs (IDIDs) or fabric binding, provided that connected channels are configured for single-byte addressing. However, you should configure IDID to ensure that domain IDs are maintained.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Verify the management IP addresses have been set up.
3. Verify the switches can be seen by your management tool.
4. Verify the switches have the correct version of Fabric OS.
5. Add feature keys, if applicable.
6. Enter the **configUpload** to save a baseline of the switch configuration.

Cascaded FICON and 2-byte addressing considerations

The following are considerations when installing a switch in a FICON environment where 2-byte addressing is used. Two-byte addressing is always used in cascaded environments but may be used in single switch- fabrics as well. Making changes to your switch or director may require scheduled downtime.

- All fabric operating parameters, such as timeout values, must be the same. If you have not made any changes outside the scope of this document, there is nothing additional to consider regarding these parameters.
- The domain IDs of all switches must be unique and insistent.
- Although not required, it will be easier to configure the security policies if the zoning matches. Configuration, connecting the ISLs, and ensuring that the switches and directors have merged into a fabric, will also make the process of setting the security attributes much easier.

Configuring switched point-to-point FICON

Use the worksheet in Appendix A, "Configuration Information Record," to record your configuration information. These steps assume you have used your hardware reference manual to perform the initial setup of the switch and have performed all the steps from "Preparing a switch for FICON" on page 17.

CAUTION

Configuring the switch for FICON is a disruptive process. The switch must be disabled to configure switch parameters.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **switchDisable** command. You will need to disable the switch to access all the switch parameters.
3. Configure the switch and chassis name, if applicable.
4. Set the routing policy to port-based routing (aptPolicy 1) by entering the **aptPolicy** command.

   The recommended best practice is to use port-based routing.

   In addition, if FICON Emulation features (IBM z/OS Global Mirror or Tape Pipelining) are enabled on an FCIP Tunnel in the switch, aptPolicy 1 must also be used.
5. Configure Dynamic Load Sharing.

   The recommended best practice is to enable Dynamic Load Sharing (DLS); however, DLS is only supported when Lossless is enabled.

   - To enable Lossless with DLS, use the **dlsSet --enable –lossless** command.
   - If Lossless will not be used, use the **dlsReset** command.

NOTE
If Lossless DLS is not enabled with Lossless DLS, the routing policy must be port-based routing (aptPolicy 1).

6. Set In-Order Delivery using the **iodSet** command.
7. Configure the switch parameters using the **configure** command and enter the responses shown in Table 2 when prompted. (Items in italics are top-level parameters.)

TABLE 2 FICON switch parameters

Parameter	Response	Comment
Fabric parameter	Yes	Prompts for the fabric parameters.
Domain		The domain ID is the switch address. The recommended best practice is to set the switch address and switch ID to be the same. The domain ID is entered in decimal so a switch address of hexadecimal 0x22 would have a domain ID of decimal 34.
R_A_TOV	10000	Do not change. Resource Allocation Time Out Value (RA_TOV)

TABLE 2 FICON switch parameters (Continued)

Parameter	Response	Comment
E_D_TOV	2000	The E_D_TOV is a timeout value entered in milliseconds. It should remain at 2 seconds (2000) unless connected to extension equipment. In some cases, when connecting to extension equipment, such as the Brocade 7800, it needs to be set to 5 seconds (5000). This field should only be changed after consulting a Brocade Certified Fabric Professional.
WAN_TOV	0	
MAX HOPS	7	This parameter should not be confused with the one-hop FICON cascading limitation. There are configurations that are more than one hop because more than two domain IDs are used in the path that fit within the IBM support limitation of “one hop.”
Data field size	2112	Do not change.
Sequence level switching	0	Do not change.
Disable device probing	0	Do not change.
Suppress Class F traffic	0	Do not change.
Per-frame route priority	0	Do not change.
Long-distance fabric	0	Do not change. The recommended best practice is to configure individual ports for long distance when cascading at extended distances.
Insistent Domain ID mode	Yes	The recommended best practice is to set the domain ID to be insistent. Setting the insistent domain ID is required for 2-byte addressing.
Virtual Channel parameters	No	Do not change.
F-Port login parameters	No	With Fabric OSv6.1.0 and later, it is not necessary to make any changes to F_Port login parameters. The only other reason to answer yes (y) to this prompt is if NPIV is being used and there is a need to change the default number of NPIV logins.
Maximum logins per switch		Change this only if NPIV is being used and the number of fabric logins will exceed the default or there is a need to limit the number of logins.
Maximum logins per port		Change this only if NPIV is being used and the number of port logins will exceed the default or there is a need to limit the number of logins.
Maximum logins per second		For Fabric OS v6.1.0b and later – Do not change. Leave at default. **NOTE:** The default value is incorrectly shown as 0.
Login stage interval		Do not change.
Zoning operation parameters	No	
RSCN transmission mode	No	
Arbitrated Loop parameters	No	
System services	No	

TABLE 2 FICON switch parameters (Continued)

Parameter	Response	Comment
Portlog events enable	No	
SSL attributes	No	
RPCD attributes	No	
cfgload attributes	No	
Web Tools attributes	No	
System	No	

8. Enter the **switchEnable** command to set the switch online.
9. Enter the **trackChangesSet** command to enable or disable the track-changes feature and to configure the SNMP-TRAP mode.
10. Enter the **fabricPrincipal** command on the switch you want to be the principal switch.

    In cascaded fabrics, only one switch should be the principal. In core-edge designs, the director class switch should be the principle.
11. Enter the **portCfgSpeed** command to configure port speeds.

    By default, all ports are configured to auto-negotiate. Normally, the only time the port configuration is changed is when connecting to 1 Gbps ports. Some DWDM ports are known not to auto-negotiate well. Furthermore, although older 1 Gbps FICON channels log in correctly, they will generate errors, so the speed should be forced to 1 Gbps with 1 Gbps FICON channels.

    NOTE
    8 Gbps ports will not auto-negotiate to 1 Gbps and cannot be configured for 1 Gbps.
12. Enter the **portCfgLongDistance** command for ports with fiber connections exceeding 10 km.

    For ports with fiber connections exceeding 10 km, configuring the port for long distance mode increases the number of buffer-to-buffer (BB) credits available on that port. If you have any Extended Fabrics links, enable VC translation link initialization to stabilize them. Refer to the *Fabric OS Administrator's Guide* for details on this option of the **portCfgLongDistance** command.
13. Enter the **supportShowCfgEnable ficon** command to turn on logging of FICON information.
14. Enter the **defZone --noaccess** command to disable the default zone.
15. Configure zoning for your fabric.

    Follow standard FCP zoning practices. For more information on zoning, refer to the administrator's guide for your management tool.
16. Enter the **statsClear** command to clear port statistics.
17. Enter the **switchShow** command to verify that the switch and devices are online.
18. Enter the **ficonShow rnid** command to verify that the FICON devices are registered with the switch. Enter this command only if fabric binding is enabled; otherwise, channels will be attached as invalid.

19. Enter the **ficonShow lirr** command to verify that the FICON host channels are registered to listen for link incidents. Enter this command only if fabric binding is enabled; otherwise, channels will be attached as invalid.

    Refer to "FICON commands" on page 13 for details about using FICON CUP.

20. Enter the **configUpload** command to save your FICON configuration.
21. Enter the command appropriate for your environment:
    - If you do not have access to an FTP server, use a Telnet session that can log console output and enter the **supportShow** command to save a FICON baseline.
    - If you have access to an FTP server, enter the **supportSave** command to save the FICON baseline of your switch.
22. Take the appropriate action based on your configuration:
    - If you have a cascaded configuration, continue configuring your switches using the instructions in "Configuring cascaded FICON" on page 21.
    - If you have and plan to use a CUP license, continue configuring your switches using the instructions in "Configuring FICON CUP" on page 31.
    - If you have a switched point-to-point configuration, you have completed the switch configuration.

Configuring cascaded FICON

In addition to performing the steps listed in "Configuring switched point-to-point FICON" on page 18, you also need to perform the following steps to configure cascaded FICON.

CAUTION

Configuring the switch for FICON is a disruptive process. The switch must be disabled to configure switch parameters. This procedure must be followed prior to channels joining the fabric.

1. Perform the following actions for each switch:
    a. Enable the IDID mode using the Fabric OS **configure** command. For details on enabling the IDID mode, refer to "Enabling insistent domain ID" on page 16.
    b. Set the domain ID. It is highly recommended that the switch ID used in HCD and IOCP be the same as the switch address in hexadecimal. All switches ship from the factory with a default domain ID of 1. The best practice is to use something other than 1 so that a new switch can be added to the fabric without changing the domain ID.
2. Use the **secPolicyCreate** command to configure the SCC policies on all switches to limit connectivity to only the switches in the selected fabric.

    ```
    switch:admin> secPolicyCreate SCC_POLICY, member;...;member
    ```

    In the command syntax, *member* indicates a switch that is permitted to join the fabric. Specify switches by WWN, domain ID, or switch name. Enter an asterisk (*) to indicate all the switches in the fabric. To create a policy that includes all the switches in the fabric:

    ```
    switch:admin> secPolicyCreate SCC_POLICY "*"
    ```

3. Save or activate the new policy by entering either the **secPolicySave** or the **secPolicyActivate** command. If neither of these commands is entered, the changes are lost when the session is logged out. To activate the SCC policy, enter the following command:

   ```
   switch:admin> secPolicyActivate
   ```

4. Enter the **fddCfg** command to enable ACL Fabric Wide Consistency Policy and enforce a strict SCC policy

   ```
   switch:admin> fddcfg --fabwideset "SCC:S"
   ```

5. Connect and enable channel and control unit (CU) devices. The Query for Security Attributes (QSA) response to the channel indicates that the fabric binding and IDID are enabled.

FICON and FICON CUP in Virtual Fabrics

For FICON CUP, FICON Management Server (FMS) mode is enabled on the logical switch and not the chassis. For example, in a Virtual Fabrics environment on the Brocade 5100 switch and the Brocade DCX and DCX-4S, one would set CUP on each logical switch (currently limited to four logical switches per chassis).

There are two different addressing modes to provide extended functionality in dynamically created partitions.

- Flat or 10-bit addressing mode
- 256-area addressing mode

Flat addressing mode

Flat or 10-bit addressing mode is the default mode for all logical switches created in the Brocade DCX and DCX-4S enterprise-class platforms. This allocates 10-bit areas by default and is not supported in FICON environments.

256-area addressing mode

The 256-area limit mode allows the partition to be configured for 8-bit addressing, rather than the default 10-bit addressing. Each port in this partition is given a unique area represented by the middle 8 bits of the PID.

Because flat addressing mode allocates 10-bit areas by default, 256-area addressing mode is used to support FICON in dynamically created partitions.

Use the fabric parameters of the **configure** command to enable the 256-area addressing mode. There are three options for the 256 area addressing mode as follows:

- Mode 0 - default mode

  The partition is configured for 10-bit addressing. Disable this mode for FICON environments using modes 1 and 2.

- Mode 1 - zero-based

  8-bit area assignments are made as ports are added to the logical switch, starting at area 0x00. FICON CUP port addresses will correspond to these 8-bit areas. You can change these area assignments using the **portAddress –bind** command.

- Mode 2 - port-based

  8-bit area assignments are made, and the area assignments will be related to the physical location of the port. FICON CUP port addresses will correspond to these 8-bit areas. These addresses are fixed and cannot be changed. Mode 2 is sometimes called “fixed” addressing and is applicable to a default switch enabled for Virtual Fabrics on a DCX platform only. Mode 2 is supported only in logical switch when a 48 port-blade is not present.

Mode 1 example

The following example illustrates mode 1, where port addresses are assigned in increasing order.

```
Enable a 256 Area Limit: (0..1) [1]
```

In this mode, the area field of the PID is allocated dynamically to the F_Ports, FL_Ports, EX_Ports, and E_Ports up to a maximum of 256 areas.

Changing port address numbering

In mode 1, as ports are assigned to the logical switch, they are assigned port addresses in an increasing manner. You can change the port address numbering using the **portAddress** command, Use this command to bind the 16-bit address to the lower two bytes of a port 24-bit Fibre Channel address.

```
switch:admin> portaddress --bind [slot/]port [16-bit-PID] [--auto]
```

Refer to the *Fabric OS Command Reference Manual* for details on this command.

NOTE
The **portAddress --bind** command is not supported with the **portSwap** command.

The *–auto* option enables autobinding on the specified port. If the auto feature is enabled, the area field of the PID address is bound to a single port. Only the high order 8 bits of the 16-bit area field in the PID address specified in the **portAddress** command are used. Following is an example using this command:

```
switch:admin> portaddress --bind 12/28 0200 –auto
```

This command results in a port that displays as the following.

```
Index Slot Port Address
=======================
252   12   28   3e0200
```

Port addresses that have not been assigned to a logical switch will appear as “uninstalled” in the PIB’s Port Descriptor.

Changing the addressing mode

Changing the addressing mode can have serious implications for the FICON user. After changing the addressing mode, the following actions occur:

- Physical ports can receive new area assignments.
- Port addresses that are referenced in an IOCDS gen can be associated with entirely new physical ports.

To change the addressing mode, use the following procedure.

NOTE
To access all parameters controlled by the **configure** command, you must disable the switch. Any configuration change to a logical switch that requires disabling the switch also requires disabling FMS mode.

1. Disable FMS mode using the **ficonCupSet fmsmode disable** command.
2. Disable the switch using the **switchDisable** command.
3. Change the address mode using the **configure** command

   The **configure** command runs in interactive mode and presents you with a series of hierarchical menus. To change the address mode, select the **Fabric parameters** menu, then select the **Enable a 256 Area Limit** field and enter appropriate option values. Refer to the *Fabric OS Command Reference Manual* for details.
4. Enable the switch using the **switchEnable** command.
5. Enable FMS mode using the **ficonCupSet fmsmode enable** command.

For more information on these Fabric OS commands, refer to the *Fabric OS Administrator's Guide*.

Moving ports to a logical switch

Ports moved into a logical switch will have the following states based on the Active=Saved (ASM) bit setting:

NOTE
You cannot issue the **portCfgPersistentDisable** command if FMS mode is enabled. When FMS mode is enabled use the **portDisable** command.

- If the ASM bit is on and the port is blocked in the internal program load (IPL) file, the port becomes persistently disabled. The port displays as persistently disabled through the **portCfgPersistentDisable** command and remains blocked in the IPL file.
- If the ASM bit is *on* and the port is unblocked in the IPL file, the port becomes persistently disabled. The port displays as persistently disabled through the **portCfgPersistentDisable** command, but is blocked in the IPL file.
- If the ASM bit is off and the port is blocked in the IPL file, the port will become persistently disabled. The port displays as persistently disabled through the **portCfgPersistentDisable** command and remains blocked in the IPL file.
- If the ASM bit is off and the port is unblocked in the IPL file, the port will become persistently disabled. The port does not display as persistently disabled through the **portCfgPersistentDisable** command and remains unblocked in the IPL file.

Clearing the FICON management database

Perform the following steps to clear RLIR and RNID records from the FICON management database.

1. Connect to the switch and log in as admin.
2. Enter **ficonClear rlir** to remove all the RLIR records from the local RLIR database.

3. Enter **ficonClear rnid** to remove all the RNID records marked “not current” from the local RNID database.

Chapter

Configuring FICON CUP

3

In this chapter

- Control Unit Port overview 27
- Port and switch naming standards for FMS 30
- Configuring FICON CUP 31
- Configuring FICON CUP in Virtual Fabrics 32
- Determining physical port assignment 33
- FMS mode and FICON CUP 34
- Mode register bit settings 37
- Setting the MIHPTO value 40
- Persistently enabling and disabling ports for CUP 40

Control Unit Port overview

The Control Unit Port (CUP) provides an interface defined by IBM that defines the Channel Command Words (CCW) that the FICON host can use for managing the switch. The protocol used is the IBM version of the ANSI FC-SB3 single-byte command code specification, which defines the protocol used for transporting CCWs to the switch, and for the switch to direct data and status back,.CUP is an optional licensed feature.

The CUP provides an interface for host in-band management and collection of FICON director performance metrics using the RMF 74-7 record, more commonly known as the FICON Director Activity Report. Host-based management programs manage the FICON directors and switches by sending commands to the switch Control Unit defined in the IOCDS and Hardware Configuration Definition (HCD). A FICON director or switch that supports CUP can be controlled by one or more host-based management programs or director consoles. Control of the FICON directors can be shared between these options. There are 39 CUP commands, or CCWs, for monitoring and control of the FICON director functions. CUP commands are oriented towards management of a single switch, even though the use of CUP in a cascaded FICON environment is fully supported.

NOTE
The CUP port address will always be xxFExx. Port Addresses xxFE and xxFF are unavailable to assign to physical ports when FMS is enabled.

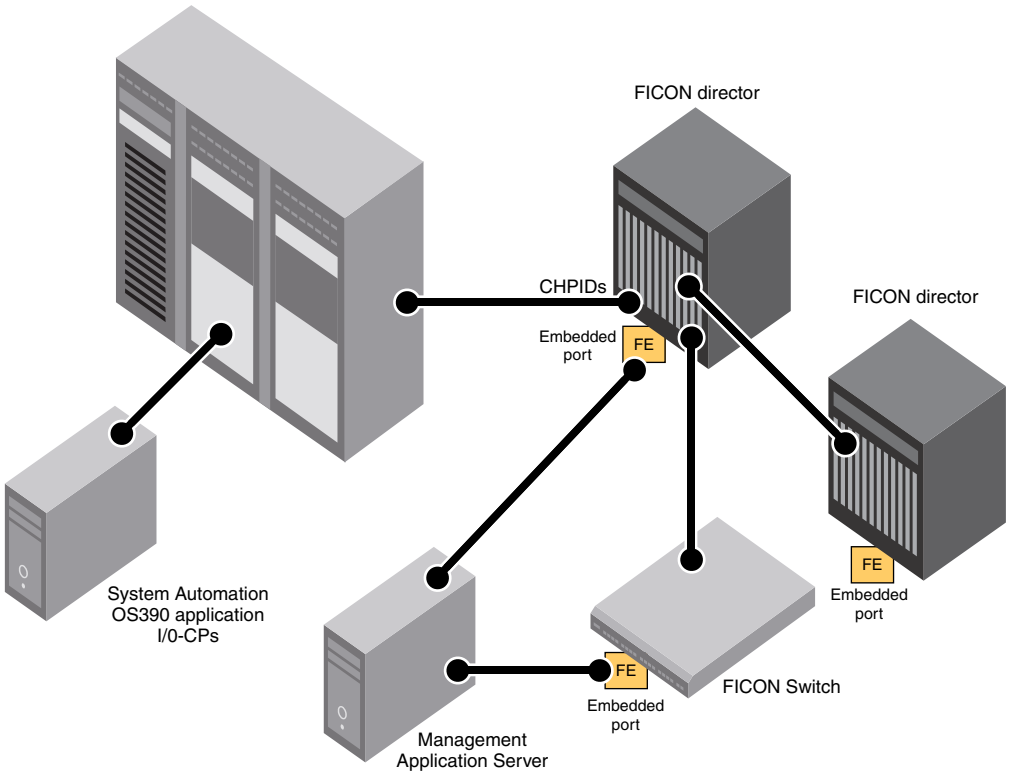


FIGURE 9 FICON CUP

Figure 9 is a simplified representation of a FICON environment and how CUP fits into that environment. FICON directors with FMS enabled use port address “FE” as the embedded internal port for host connectivity to the CUP, and port address “FF” is reserved. Therefore addresses “FE” and “FF” cannot be used for assignment to physical ports when FMS is enabled. If physical ports have been assigned addresses “FE” or “FF” by default prior to enabling FMS, they will be automatically disabled when FMS is enabled. If there are active devices connected to the ports, then the ports must first be disabled manually in order to enable FMS. Because these ports are not available after enabling FMS mode, you should first move any fiber connected to either of them to another free port. On logical switches with Dynamic Addressing mode, such ports may be reclaimed for external connections by binding a new address to the port, if unused addresses are available. Ports that are disabled for having addresses “FE” or “FF” when FMS is enabled are not eligible for port swapping. In a FICON environment, only one RMF LPAR be configured to poll the CUP for port statistical counter data in order to minimize contention for the CUP device. Host contention for access to the CUP can lead to missing interrupts, potentially causing the host to box the device. It is a best practice however to have more than one CHPID defined as a path to the CUP in order to ensure redundancy for host-to- CUP connectivity.

FICON CUP restrictions

The following restrictions apply to Brocade FICON directors having at least 256 ports when FMS mode is enabled and when host applications are used for inband monitoring and management of the switch:

- *FICON Management Server mode* (FMS mode) must be enabled on the switch to enable CUP management features. When this mode is enabled, Fabric OS prevents configuration requests from out-of-band management interfaces from interfering with host in-band configuration requests by serializing access to switch parameters.

  ATTENTION
  Once FMS mode is enabled, you cannot bind FE/FF to any ports using either the **portAddress** or **wwnAddress** commands.

- The switch is advertised to the mainframe by the CUP as having a specific number of ports, which is based on the hardware platform. The maximum supported switch size is 256 ports.

  The addresses FE/FF are not components of the Allow/Prohibit Matrixes (as they are called in the Brocade Network Advisor) or CUP Configurations (as they are referred to in Web Tools), because the Prohibit Dynamic Connectivity Masks (PDCMs) for these two ports are defined architecturally and cannot be modified by the user.

  The Port Address Name for the internal FE port can be read by the host, and corresponds to the switchname that is set for the switch. The switchname may be modified by the host, with the limitation that the host may write EBCDIC characters that cannot be converted directly to ASCII for display in the GUI or CLI management interfaces. Such characters will be converted to periods for these displays.

- The FC8-48 blade supports FICON attachment in switches or logical switches. In the Brocade DCX, the FC8-48 is only supported in a logical switch configured for zero-based addressing.
- Addresses 0xFE and 0xFF are not available for external connections. Before enabling FMS mode, you must manually disable physical ports associated with 0xFE and 0xFF if there is an active device connected to these ports. Otherwise, these ports disable automatically when FMS is enabled. Because these ports are not available after enabling FMS mode, you should first move any fiber connected to either of them to another free port.

CUP configuration recommendations

The following are recommendations for setting up FICON CUP:

- Device Type: 2032

  Although IBM has developed new machine types for the switches and directors, all directors and switches regardless of model or manufacture should be configured as 2032.

- Paths

  Define at least two CHPIDs as paths to the CUP in the IOCDS Control Unit statement for the switch to ensure redundancy for host connectivity.

- RMF 74-7 statistics gathering

So as not to overwhelm the CUP, the recommended best practice in a sysplex environment is to disable FICON switch statistics (RMF polling) on all but one host system that has inband access to the CUP. If no FICON statement is specified, the system will gather switch statistics by default so FICON switch statistics should be disabled on all but the system intended to gather statistics.

- Missing Interrupt Handler (MIH)

  Set the MIHPTO to three minutes (180 seconds).

FICON CUP zoning and PDCM considerations

The FICON PDCMs control whether or not communication between a pairs ports in the switch is prohibited or allowed. PDCMs are a per-port construct. Each port on the switch has its own PDCM that defines whether communication is allowed between that particular port, and each of the other ports in the switch, including itself. The Allow/Prohibit Matrix presents a matrix that allows you to set and clear the PDCMs for all external ports. If there are any differences between restrictions set up with Brocade Advanced Zoning and PDCMs, the most restrictive rules are automatically applied.

FMS must be enabled for the Allow/Prohibit matrix to be operational, and there must be an active zoning configuration. (D,I) zoning is recommended for FICON, but is not specifically required.

If Brocade Advanced Zoning is in use, refer to the *Fabric OS Administrator's Guide* for more information on configuration.

Port and switch naming standards for FMS

FMS and the FICON Programming Interface employ 8-bit EBCDIC characters in port address names and switch names. Fabric OS employs 7-bit characters, therefore when FMS mode is enabled, all characters greater than 0x40 and not equal to 0xFF (EBCIDC code page 037 [0x25] - refer to Appendix B, "EBCDIC Code Page") are allowed iport address names, and it is possible for a channel to set a name with nonprintable characters. If a name contains nonprintable characters, those characters are displayed as dots (...). The following characters are also displayed as dots: semicolon (;), comma (,), equal sign (=), and at sign (@).

FICON CUP Fabric OS commands

Table 3 summarizes the Fabric OS CLI commands that can be used for managing FICON fabrics. For detailed information on these commands, see the *Fabric OS Command Reference*.

TABLE 3 Fabric OS commands related to FICON CUP

Command	Description
ficonCupset fmsmode	Sets FICON Management Server mode on or off for the switch.
ficonCupset crp	Sets the CUP Asynchronous Event Reporting Path.
ficonCupset MIHPTO	Sets the Missing Interrupt Handler Primary Timeout value.
ficonCupset modereg	Sets the mode register bits for the switch.
ficonCupShow lp	Displays the host logical path information for the CUP.
ficonCupShow MIHTPTO	Displays the Missing Interrupt Handler Primary Timeout value.

TABLE 3 Fabric OS commands related to FICON CUP

Command	Description
ficonCupShow fmsmode	Displays the FICON Management Server enabled/disabled state for the switch.
ficonCupShow modereg	Displays the mode register bit settings for the switch.

Configuring FICON CUP

To set up FICON CUP, use the following procedure and be sure to perform the steps in the order indicated.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Verify that the switch or director has been set up according to the instructions in "Configuring switched point-to-point FICON" on page 18, and if in a cascaded topology, "Configuring cascaded FICON" on page 21.
3. For directors with at least 256 ports installed, use the **portDisable** command to disable ports 0xFE and 0xFF.

   Refer to "Persistently enabling and disabling ports for CUP" on page 40 for more information and detailed instructions.

   Addresses 0xFE and 0xFF are not available for external connections. Note that in logical switches or in cases where port address binding or port swapping has occurred, addresses 0xFE and 0xFF are not necessarily tied to specific physical ports, such as 254 and 255. After FMS mode has been successfully enabled, these two ports remain disabled and cannot be used either as an F_Port or an E_Port. Because these ports are not available after enabling FMS mode, you should first move any fiber connected to either of them to another free port.

   You must manually disable ports associated with 0xFE and 0xFF to enable FMS mode only if there is an active device connected to these ports. Otherwise, the Fabric OS will disable them automatically when FMS is enabled.

   On a Brocade DCX and DCX-4S Backbones, when Virtual Fabrics is not enabled or zero-based addressing is not used, you must disable physical ports associated with addresses 0xFE and 0xFF (if ports were assigned by default) before enabling FMS mode. Note that physical ports associated with 0xFE and 0xFF may be different in logical switches using zero-based addressing. Disable these addresses manually if there is an active device attached. If an active device is not attached to the ports, they will disable automatically when you enable FMS mode.

   NOTE
   You can only disable ports if there is a card present in the slot.

   If FMS mode is enabled in a logical switch with port-based addressing, the physical ports with addresses 0xFE and 0xFF are essentially wasted and may be used better elsewhere. This is the same for a switch with dynamic addressing where all available addresses are used, and thus no addresses are available for binding to these ports. In a logical switch where there are addresses available, you can simply bind a new address to such ports in order to make them available for external connections.
4. Enter the **ficonCupShow fmsmode** command to verify if FMS mode is disabled.

5. Take the appropriate action based on whether FMS mode is enabled or disabled:
   - If FMS mode is disabled, proceed to step 6.
   - If FMS mode is enabled, disable it using the **ficonCupSet fmsmode disable** command.

   ATTENTION
   If FMS mode is already enabled, disabling it might be disruptive to operations because ports that were previously prohibited from communicating will be allowed to do so because prohibits are no longer enforced.

   You must disable FMS mode to continue setting up CUP.

6. Install a CUP license on the switch. For more information on installing a license, refer to the *Fabric OS Administrator's Guide*.
7. Enter the **ficonCupSet fmsmode enable** command to enable FMS mode (FMS mode) on the switch.
8. Enter the **ficonCupSet modereg** command to set the mode register bits. Refer to "Mode register bit settings" on page 37 for more information.
9. Verify with the systems programmer that the CUP ports are defined properly.

   FICON ports are defined as part of the sysgen process. The z/OS systems programmer can verify if the CUP ports are defined properly.

Configuring FICON CUP in Virtual Fabrics

You can configure up to four CUP switches as logical switches in a Virtual Fabrics-enabled platform for FMS mode. A base switch cannot be configured as a FICON switch.

FICON CUP-enabled logical switches are not supported as logical fabric-capable logical switches, so FICON logical switches will not participate in the use of extended ISLs on the base switch.

You cannot have 48-or 64-port blades in the default logical switch with FMS mode enabled. Also, you cannot have chassis port numbers greater than 255 in a logical switch with FMS mode enabled.

If addresses 0xFE or 0XFF have been assigned to physical ports, those ports must be disabled.

When FMS mode is enabled and Virtual Fabrics mode is disabled, the ports on a 48-port blade are not managed through FMS mode. The ports are intended for FCP devices only.

When FMS mode is enabled and Virtual Fabrics mode is enabled, the ports on a 48-port blade are not supported to connect to either FICON or FCP (open system) devices. This is enforced starting with Fabric OS v6.3.0 and the ports on a 48-port blade are explicitly disabled in the default switch. This disabling occurs during an upgrade and insertion of the blade, where Fabric OS detects these ports in the default switch.

When FMS mode is enabled and Virtual Fabrics mode is enabled, the ports on a 48-port blade are supported in non-default logical switches for both FICON open-system device connectivity. Address mode limitations apply.

For FICON CUP, FMS mode is enabled on the logical switch and not the chassis. For example, in a Virtual Fabrics environment on the Brocade 5100 switch and the Brocade DCX and DCX-4S, one would set FMS mode independently on each logical switch. FMS mode is currently limited to four logical switches per chassis).

Each logical switch has its own configuration data, such as the initial program load (IPL) file, configuration data elements (PDCM, PIB, Port Address Names, Mode Register, Key Counter), and CUP configuration files.

Following is a summary of steps to create a logical switch using the Fabric OS commands. You can find the complete instructions for creating a logical switch in the *Fabric OS Administrator's Guide*.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Determine current logical switch configuration using the **lsCfg --show** command.
3. Define the new logical switch using the **lsCfg --create** command.
4. Enter the **setContext** command to set the context to the newly created logical switch.
5. Enter the **configure** command to configure the newly created logical switch.
6. Enter **y** at the **Fabric Parameters** prompt.
7. Assign a domain ID, as appropriate.
8. Allow XISL USE (0). This parameter must be zero (0) for FICON.
9. Set the 256 area mode. This parameter can be set to 1 or 2 for FICON CUP.

   Dynamic, or zero-based area assignment (256 Area Mode = 1), has the advantage of allowing you to use high port count (48 port) blades.

   Fixed, or port-based area assignment (256 Area Mode = 2). For this mode, you cannot add a port with an index greater than 255 to the partition. As the name implies, the default assignment is area = port.
10. Add ports to the logical switch using the **lsCfg --configure** command.
11. (Optionally - Area Mode 1) Bind a port address to the index using the following syntax:

    ```
    portaddress --bind [SlotNumber/]PortNumber <16 bit area> --auto [1|0]
    ```
12. Display switch port content using the **switchShow** command.
13. Once the logical switches are set up, install CUP on the logical switch per the instructions in "Configuring FICON CUP" on page 31.

Determining physical port assignment

The following instructions help you locate the physical port from CUP_PortAddress.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Set the context to the appropriate logical switch.
3. Enter the **switchShow** command.
4. Look for the PID in the **Address** column.
5. Read across to the **Slot** and **Port** columns.
6. Enter the **portAddress --findPID** command.

Example of locating the physical port address

```
Index Slot Port Address Media Speed State      Proto
==================================================
255   12   28   01fc00  --    N8    No_Module  Disabled
```

```
253   12   29   01fd00  --    N8    No_Module  Disabled

switch:FID2:admin> portaddress --findpid 01fc00

Index Slot Port ID
==================
252   12   28   0x 1fc00
```

FMS mode and FICON CUP

For Fabric OS 7.0 and later, a FICON CUP license is required to enable FMS mode. The FMS mode setting can be changed whether the switch is disabled or enabled. If FMS mode is changed while the switch is enabled, a device reset is performed for the control device and an RSCN is generated with PID 0xDDFE00, where 0xDD is the domain ID of the switch.

When FMS mode is enabled, the following Fabric OS commands return a “switch busy” response if they are issued when the host-based management application is performing a write operation. This *serialization* prevents interference from out-of-band management applications when a host-based management program is being used to administer the switch.

bladeDisable	bladeDisable
bladeEnable	bladeEnable
portDisable	switchCfgPersistentDisable
portEnable	switchDisable
portName	switchEnable
portShow	switchName
portSwap	switchShow

NOTE
You cannot use the **portCfgPersistentEnable** and **portCfgPersistentDisable** commands to persistently enable and disable ports when FMS mode is on. See the procedure “Persistently enabling and disabling ports for CUP” on page 40 for instructions.

Changing FMS mode from *disabled* to *enabled* triggers the following events:

- Access to switch configuration parameters is serialized.
- The active CUP configuration data, including the following, is initialized according to the IPL file:
  - Port and switch names.
  - Port “Block” and “Unblock” values.
  - PDCM values.
- Brocade Advanced Zoning, if used, continues to be in force. If there are any differences between the port-to-port connectivity restrictions defined by Brocade Advanced Zoning and those defined by PDCMs, the most restrictive rules are automatically applied.
- RSCNs are sent to devices if PDCM changes result in changes to connectivity between a set of ports that are zoned together.
- An RSCN for the CUP is generated to all mainframe FICON and FCP channels in the fabric.

Changing FMS mode from *enabled* to *disabled* triggers the following events:

- A device reset is performed on the control device.

- Prohibits are no longer enforced.
- RSCNs might be generated to some devices if PDCM removal results in changes to connectivity between a set of ports that are zoned together.
- If a given port was set to “Block” or “Unblock,” that port remains disabled or enabled.
- The switch interface for host in-band management is no longer enabled.
- An RSCN for the CUP is generated to all mainframe FICON and FCP channels in the fabric.

Displaying FMS mode

The **ficonCupShow fmsmode** command displays the FMS mode enabled/disabled state for the switch.

```
switch:admin> ficoncupshow fmsmode
fmsmode for the switch: Enabled
```

Enabling FMS mode

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter **ficonCupSet fmsmode enable.**
3. Enter the **ficonCupShow fmsmode** command to verify if FMS mode is enabled.

Disabling FMS mode

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter **ficonCupSet fmsmode disable.**
3. Enter the **ficonCupShow fmsmode** command to verify if FMS mode is disabled.

Setting up FICON CUP if FMS mode is enabled

1. Connect to the switch and log in using an account assigned to the admin role.
2. Verify that FMS mode is enabled by entering the **ficonCupShow fmsmode** command.

   ATTENTION
   If FMS mode is already enabled, disabling it might be disruptive to operation because ports that were previously prevented from communicating will now be able to do so.

3. If FMS mode is enabled, then disable it by entering the **ficonCupSet fmsmode disable** command.
4. Enter the **ficonCupShow fmsmode** command to verify if fmsmode is disabled.
5. Install the CUP license.
6. Enter the **ficonCupSet fmsmode enable** command.

7. Enter the **ficonCupShow fmsmode** command to verify if FMS mode is enabled.

FMS mode and FICON 0xFE or 0xFF addresses

0xFE and 0xFF are assigned to the CUP and cannot be associated with any physical port with FMS mode enabled. Therefore, note the following when using FMS mode:

- You must manually disable ports associated with 0xFE and 0xFF to enable FMS mode, but only if there is an active device connected to these ports. Otherwise, the Fabric OS will disable them automatically when FMS is enabled.
- Enabling FMS mode disables all ports with 0xFE and 0xFF addresses.
- If you enable FMS mode, you will get port-disable messages for physical ports with 0xFE or 0xFF FICON addresses.
- You cannot enable FMS mode when physical ports have 0xFE or 0xFF FICON addresses with live devices connected.
- Port Swapping and Blade Swapping cannot be performed when FMS mode is enabled and swapped ports have 0xFF or 0xFE FICON addresses.

Upgrade considerations

Take the CUP offline before performing an upgrade or downgrade operation. The upgrade can disrupt CUP exchanges, especially for active RMF sessions.

For Fabric OS 7.0 and laster, a FICON CUP license is required to enable FMS mode. Consider the following when using FMS mode and upgrading from Fabric OS v6.4 to v7.0:

- If using Fabric OS v6.4 and FMS mode is enabled, but a FICON CUP license was never installed:
  - You can manage the port connectivity configuration through management applications such as the Brocade Network Advisor and WebTools.
  - The Inband Management feature is not enabled.
  - After a nondisruptive upgrade from Fabric OS v6.4 to v7.0:
    - You can manage the port connectivity configuration using management programs such as the Brocade Network Advisor and Web Tools. The Web Tools mode register is accessible.
    - To enable Inband Management, you must install a FICON CUP license and disable, then re-enable FMS mode.

    NOTE
    The preceding information does not apply to the DCX-8510 as a nondisruptive upgrade is not possible.

- If using Fabric OS v6.4 and FMS mode is enabled, but a FICON CUP license was installed, then removed:
  - You can manage port connectivity through management applications such as the Brocade Network Advisor and WebTools. The Web Tools mode register is accessible.
  - Inband Management is enabled, providing you do not disable FMS mode, disable, then re-enable the switch, or power-cycle the switch.

After a nondisruptive upgrade from Fabric OS v6.4 to v7.0:

- You can manage port connectivity using the Allow/Prohibit matrix in Brocade Network Advisor and Web Tools. Note that these applications are not available unless you install a FICON CUP license. The Mode Register is accessible via WebTools and the Fabric OS commands.
- Inband management is enabled, provided you do not disable FMS mode, disable then enable the switch, or power-cycle the switch.
- If you disable FMS, a FICON CUP license is required to re-enable the feature.

Mode register bit settings

A *mode register* controls the behavior of the switch with respect to CUP itself, and with respect to the behavior of other management interfaces. The mode register bits are described in Table 4.

TABLE 4 FICON CUP mode register bits

ACP	Alternate control prohibited. Because the Fabric OS CLI, Web Tools, and Brocade Network Advisor are considered to be switch consoles, this bit has no effect on their operation. Attempts to set CUP parameters through SNMP are denied when this bit is set on. The default setting is 1 (on).
ASM	Active=Saved mode. When this bit is set on, all CUP configuration parameters are persistent, meaning that they will be saved in nonvolatile storage in the IPL file that is applied upon a cold reboot or a power cycle. The default setting is 1 (on).
DCAM	Switch clock alert mode. When this bit is set on, a warning is issued when the **date**, **tsClockServer**, or **tsTimeZone** commands are entered to set the time and date on the switch. The default setting is 0 (off).
HCP	Host control prohibited. When this bit is set on, the host is not allowed to set CUP parameters. The default setting is 0 (off).
POSC	Programmed offline state control. If the bit is set (=1), the command from the host will set the switch offline. If the bit is off (=0) the command from the host will be rejected and the switch will not go offline. The default setting is 1 (on).
UAM	User alert mode. When this bit is set on, a warning is issued when an action is attempted that will write CUP parameters on the switch. The default setting is 0 (off).

The **ficonCupShow modereg** command displays the mode register bit settings for the switch. A display of 0 indicates that the mode register bit is set to off; 1 indicates that the bit is set to on.

The following example displays all mode register bit settings for the switch. When the POSC bit=1, the FICON host is allowed to set the switch offline. The bit is set to 1 by default. If you do not want to allow the host to have permission to set the switch offline, the bit should be turned off. The state of this bit cannot be changed by the FICON host, it can only be changed through the command line.

```
switch:admin> ficoncupshow modereg
POSC  UAM  ASM  DCAM  ACP  HCP
------------------------------
   1    0    1     0    1    0
```

To display the mode register bit HCP for the switch enter the ficonCupShow command as shown in the following example:

```
switch:admin> ficoncupshow modereg HCP
HCP
0
```

FICON file access facility

The FICON file access facility (FAF) is used to store configuration files. This includes the initial program load (IPL) and other configuration files. The Fabric OS saves the IPL and all other configuration files on the switch. A maximum of 16 configuration files, including the IPL file, are supported.

You can upload the configuration files saved on the switch to a management workstation using the **configUpload** command. Data uploaded using the **configUpload** command also contains the IPL file that was current at the time the command was executed.

Refer to the *Fabric OS Administrator's Guide* for more information on the **configUpload** process.

Configuration files uploaded

When you execute the **configUpload** command, all the files saved in the file access facility are uploaded to a management workstation (there is a section in the uploaded configuration file labeled [FICU SAVED FILES] where the files are stored in an encoded format).

Configuration files downloaded with Active=Saved mode enabled

The contents of existing files saved on the switch, which are also present in the "FICON_CUP" section, are overwritten.

The files in the [FICU SAVED FILES] section of the configuration file, which are not currently on the switch, are saved on the switch.

The IPL will not be replaced because Active=Saved mode is enabled. A warning message is displayed in the event log to warn users that the IPL will not be overwritten.

Configuration files downloaded with Active=Saved mode disabled

The contents of existing files saved on the switch, which are also present in the [FICU SAVED FILES] section, are overwritten.

The files in the [FICU SAVED FILES] section of the configuration file, which are not currently on the switch, are saved on the switch.

The IPL is replaced because Active=Saved mode is disabled.

Sample IOCP configuration file

The channel subsystem controls communication between a configured channel, the control unit, and the device. The I/O Configuration Data Set (IOCDS) defines the channels, control units, and devices to the designated logical partitions (LPARs) within the server; this is defined using the Input/Output Configuration Program (IOCP). The IOCP statements are typically built using the hardware configuration definition (HCD). The interactive dialog is used to generate your Input/Output Definition File (IODF), invoke the IOCP program, and subsequently build your production IOCDS.

Each FICON director in a fabric must have a unique domain ID and a unique switch ID. The switch ID used in the IOCP definitions can be any value between x'00' to x'FF'. The domain ID range for directors is hex x'01' to x'EF' or decimal 1 to 239. When defining the switch IDs in the IOCP definitions, ensure that you use values within the FICON director's range.

The switch ID has to be assigned by the user and must be unique within the scope of the definitions (IOCP and HCD).

The domain ID is assigned by the manufacturer and can be customized to a different value. It must be unique within the fabric.

Brocade recommends that the switch ID (in IOCP or HCD) be set to the same value as the domain ID of the FICON director, which is defined to the FICON director at installation time. This simplifies the configuration and reduces confusion by having a common designation across all definitions.

For more information on switch numbering, refer to the IBM publication, *FICON® Implementation Guide* (SG24-6497-00).

In the following sample IOCP configuration file, the UNIT value for FICON CUP definitions is **2032** for any FICON director regardless of vendor or platform. All Brocade switches require **UNIT=2032** for the CUP definition. All Domain IDs are specified in hex values in the IOCP (and not in decimal values).

```
*--------------------------------------------------------------------
* Brocade Domain_ID=0x3c0000
*--------------------------------------------------------------------
 CNTLUNIT CUNUMBR=0D8,UNITADD=00,UNIT=2032,
              PATH=(50,51),
              LINK=(61FE,61FE)
 IODEVICE ADDRESS=(0D8,1),CUNUMBR=0D8,UNIT=2032,STADET=Y,UNITADD=00
*--------------------------------------------------------------------
 CNTLUNIT CUNUMBR=0D9,UNITADD=00,UNIT=2032,
              PATH=(8A,8B),
              LINK=(22FE,22FE)
 IODEVICE ADDRESS=(0D9,1),CUNUMBR=0D9,UNIT=2032,STADET=Y,UNITADD=00
*--------------------------------------------------------------------
* Brocade Domain_ID=0x190000
*--------------------------------------------------------------------
*
 CNTLUNIT CUNUMBR=0DB,UNITADD=00,UNIT=2032,
              PATH=(5A,5B),
              LINK=(25FE,25FE)
 IODEVICE ADDRESS=(0DB,1),CUNUMBR=0DB,UNIT=2032,STADET=Y,UNITADD=00
*
*--------------------------------------------------------------------
```

Setting the mode register bits

Consider the following when changing mode register bits:

- The UAM bit can only be set by host programming.
- All mode register bits except UAM are saved across power on/off cycles; the UAM bit is reset to 0 following a power-on.
- Mode register bits can be changed when the switch is offline or online. If the ACP or HCP bits are changed when the switch is online, they will take effect any time between the completion of the current command and the end of the CCW command chain (or the next alternate manager operation).

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **ficonCupSet modereg** command to set the FICON CUP mode register bits for the local switch.

Example of setting the mode register bit HCP to off:

```
switch:admin> ficoncupset modereg HCP 1
Mode register bit HCP has been set to 1.
```

Example of setting the mode register bit ACP to on:

```
switch:admin> ficoncupset modereg ACP 1
Mode register bit ACP has been set to 1.
```

Setting the MIHPTO value

You can set missing interrupt handler primary timeout (MIHPTO) value and this determines how long the channel will wait before timing out an expected response from the CUP. This value is part of the data returned to the host when it reads the configuration data, but the host is under no obligation to adhere to this value. The actual value that the host will use before detecting a timeout can be set by the system programmer (overriding the value returned by the switch).

The **ficonCupSet MIHPTO** command can be used to increase, decrease, or display the MIHPTO value that the CUP returns to the host when configuration data is read. Changing the MIHPTO value requires that the CUP control device be varied offline from the host, as the host will not automatically be notified when the value is changed. The host will normally read the new value, using the Read Configuration Data command, when the CUP is varied back online.

The MIHPTO setting will persist across reboots, POR, and failovers. Setting this value to the upper end of the time range will allow the CUP more time to process requests during intervals of peak usage, without causing the host to detect timeouts. It is recommended that the value be set to 180 (default) seconds.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **ficonCupSet MIHPTO** command and set the value between 15 and 600.

Persistently enabling and disabling ports for CUP

When FMS mode is enabled, you cannot use the **portCfgPersistentEnable** and **portCfgPersistentDisable** commands to persistently enable and disable ports. Instead, use the following procedure.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **ficonCupShow modereg** command to display the mode register bit settings.
3. Verify that the ASM bit is set on (1).
4. If the ASM bit is set off (0), enter the **ficonCupSet modereg asm 1** command to set it on.

   In the following example, the ASM bit is shown as being off and then it is set to on.

```
switch:admin> ficoncupshow modereg
POSC  UAM  ASM  DCAM  ACP  HCP
------------------------------
   1    0    0     0    1    1

switch:admin> ficoncupset modereg ASM 1
Active=Saved Mode bit is set to 1.
```

5. Use the **portEnable** and **portDisable** commands to enable and disable ports as necessary.

   The ports remain enabled or disabled after a switch reboot.

   ```
   switch:admin> portenable 1/1
   ```

Chapter

4

Administering FICON Extension Services

In this chapter

- FICON emulation overview 43
- FCIP configuration requirements for FICON extension 48
- Configuration requirements for switches and directors 48
- Configuring FICON emulation 50
- Modifying FICON emulation 53
- Displaying FICON emulation performance statistics. 53

FICON emulation overview

FICON emulation supports FICON traffic over IP WANs using FCIP as the underlying protocol. FICON emulation can be extended to support performance enhancements for specific applications through use of the following licensed features:

- IBM z/OS Global Mirror (formerly eXtended Remote Copy or XRC)
- FICON Tape Emulation (tape read and write pipelining)

The 4Gbps FR4-18i blade uses the following licenses:

- High-Performance Extension over FCIP/FC

  Allows creation of tunnels.
- FICON Tape

  Allows FICON Tape emulation.
- IBM z/OS Global Mirror

  Allows FICON IBM z/OS Global Mirror emulation.
- Brocade Accelerator for FICON

  Enables both FICON tape emulation and IBM z/OS Global Mirror emulation. One license must be used per unit or blade.

The 8Gbps platforms (7800 or FX8-24) use the following licenses.

- Advanced FICON Acceleration (FTR_AFA)

  Allows interoperability for the following features and products:

  - Prizm FICON to ESCON converter and ESBT Bus/Tag Interface Module for Prizm from Optica Technologies, Inc.
  - Write and read tape pipelining
  - Teradata emulation
  - IBM z/OS Global Mirror emulation.

The Advanced FICON Acceleration license contains the following options:

- Capacity 1
- Consumed 1
- Configured Blade Slots 1

This is a slot-based license for the FX8-24 and 7800.

- Advanced Extension (FTR_AE)

  Required for multiple-circuit tunnels, FCIP Trunking, Adaptive Rate Limiting, and other FCIP features. This is not required for FICON Acceleration features, but multiple circuits would be used in a FICON emulation environment. This is a slot-based license for the FX8-24 and 7800.

  - Capacity 1
  - Consumed 1
  - Configured Blade Slots 1

ATTENTION
Use the **licenseShow** command to verify the licenses are installed on the hardware at both ends of the FCIP tunnel. For slot-based licenses, use the **licenseslotcfg –show** command to display all slot-based licenses in a chassis.

IBM z/OS Global Mirror emulation

The IBM z/OS Global Mirror emulation (formerly eXtended Remote Copy or XRC) application is a direct attached storage device (DASD) application that implements disk mirroring, as supported by the disk hardware architecture and a host software component called System Data Mover (SDM). Within this application a specific application channel program invokes a well constrained type of channel program called a Read Record Set (RRS) channel program. This channel program is used to read only updates to disk volumes (record sets) after they have been brought into synchronization with the aim of writing only record updates to a mirrored volume. The RRS channel program accesses primary volumes from a remote host for the purpose of reading these record sets (updates) that is supported by IBM z/OS Global Mirror emulation. The emulation feature thus allows the primary volume to be located at a distance from its mirrored secondary without encountering performance degradation associated with a specific FICON facility called IU pacing.

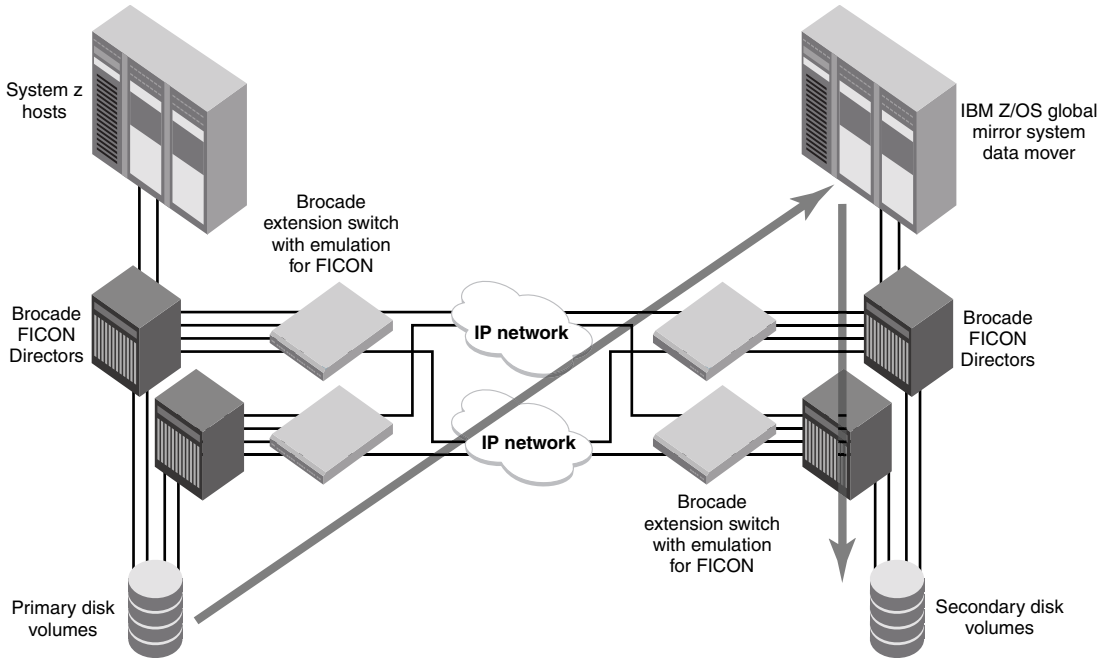

System z hosts
IBM Z/OS global mirror system data mover
Brocade extension switch with emulation for FICON
Brocade FICON Directors
IP network
IP network
Brocade FICON Directors
Brocade extension switch with emulation for FICON
Primary disk volumes
Secondary disk volumes

FIGURE 10 IBM z/OS Global Mirror emulation

Figure 10 shows how the primary volume and the secondary mirrored volume may be geographically distant across an IP WAN. Updates to the primary disk volumes are completed by the production applications and then staged in control unit cache to be read by the SDM. SDM then writes the updates to the secondary volumes. The latency introduced by greater distance creates delays in anticipated responses to certain commands. The FICON pacing mechanism may interpret delays as an indication of a large data transfer that could monopolize a shared resource and react by throttling the I/O. IBM z/OS Global Mirror emulation provides local responses to remote hosts, eliminating distance related delays. You can use the Brocade 7800, an FR4-18i, or an FX8-24 blade with FICON emulation.

Tape emulation

Tape emulation (also called tape pipelining) refers to the concept of maintaining a series of I/O operations across a host-WAN-device environment and should not be confused with the normal FICON streaming of CCWs and data in a single command chain. Normally tape access methods can be expected to read data sequentially until they reach the end-of-file delimiters (tape marks) or to write data sequentially until either the data set is closed or an end-of-tape condition occurs (multi-volume file). The emulation design strategy attempts to optimize performance for sequential reads and writes, while accommodating any other non-conforming conditions in a lower performance non-emulating frame shuttle. Since write operations can be expected to comprise the larger percentage of I/O operations for tape devices (for archival purposes) they are addressed first.

Tape Write Pipelining

FICON Tape Write Pipelining (refer to Figure 11)improves performance for a variety of applications when writing to tape over extended distances. FICON Tape Write Pipelining locally acknowledges write data records, enabling the host to generate more records while previous records are in transit across the IP WAN. If an exception status is received from the device, the writing of data and emulation is terminated.

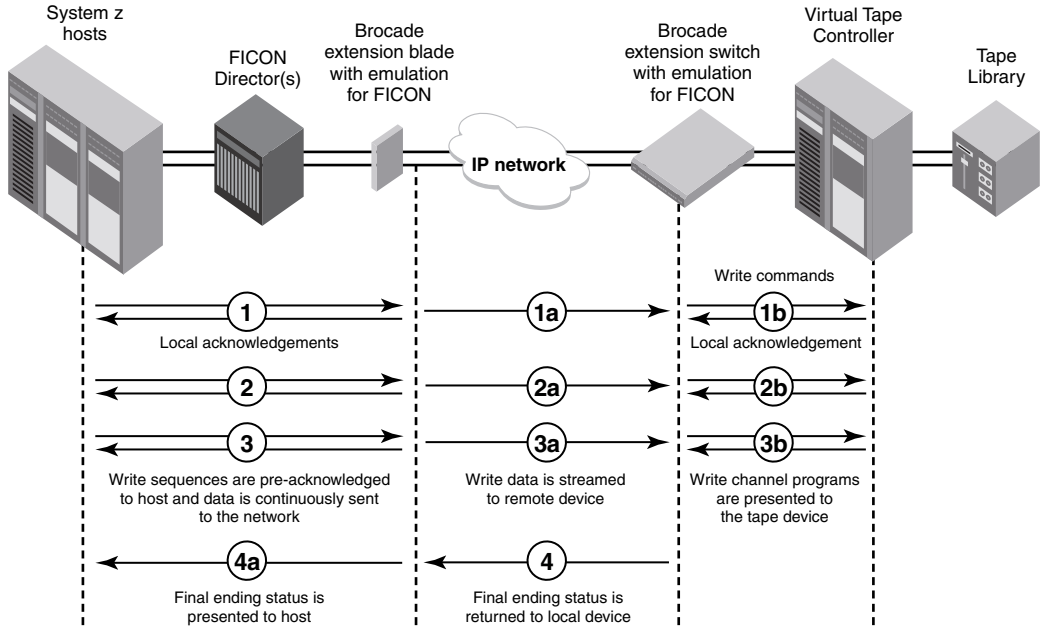


FIGURE 11 Tape Write Pipelining

Tape Read Pipelining

FICON Tape Read Pipelining (Figure 12 on page 47) improves performance for certain applications when reading from FICON tape over extended distances. FICON Tape Read Pipelining reads data on the tape directly from the tape device. Reading of the tape continues until a threshold is reached. The buffered data is forwarded to the host in response to requests from the host. When the host sends the status accept frame indicating that the data was delivered, the read processing on the device side credits the pipeline and requests more data from the tape. If an exception status is received from the device, the reading of data and emulation is terminated.

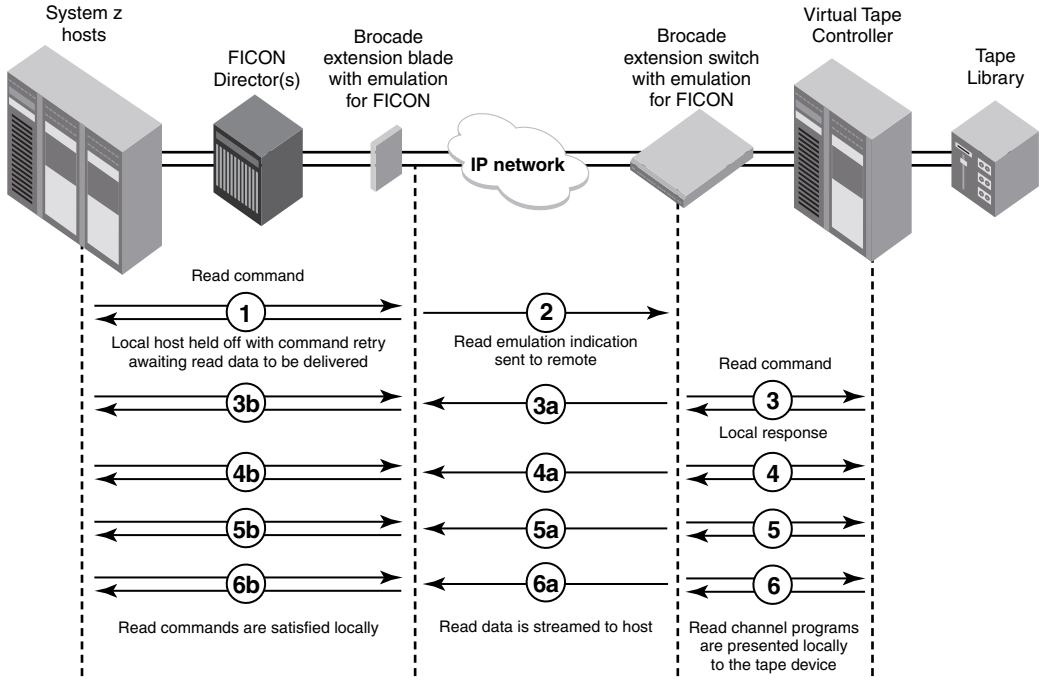


FIGURE 12 Tape Read Pipelining

FICON and ESCON conversion support

The 7800 switch and FR4-18i blade can operate with Prizm FICON to ESCON converter and ESBT Bus/Tag Interface Module for Prizm from Optica Technologies, Inc. This provides FICON tape emulation when connecting to ESCON and to bus and tag devices including 3480, 3490, and 3590 controllers. The discovery of these devices is automatic when FICON emulation is enabled on an FCIP tunnel.

Teradata emulation

Teradata emulation reduces latency on links to Teradata warehouse systems caused by WAN propagation delays and bandwidth restrictions. It accomplishes this by processing selected FICON commands for associated control, data, and status responses. FICON Teradata Emulation is only supported between FICON Channels and FICON Teradata controllers.

For write commands, control and status frames are generated for the host side of the WAN in order to pipeline write commands over the same or multiple exchanges. Such pipelined write commands and their data are queued at the device side of the WAN for asynchronous transfer to the device.

For read operations received by the device side of the WAN, a number of anticipatory read commands are autonomously generated and transferred to the device. The data and status associated with such commands are sent to the host side of the WAN and queued in anticipation of host generated read commands.

FICON Emulation for Teradata sequences over an FCIP Tunnel is controlled by using FICON emulation feature flags in the **portcfg fciptunnel** command associated with the FCIP Tunnel. Refer to "Configuring emulation on the 7800 switch and FX8-24 blade" on page 51.

Platforms supporting FICON extension over IP

Fabric OS supports SAN extension between Brocade 7800 extension switches, FR4-18i blades, and FX8-24 blades.

- The Brocade FR4-18i blade has 16 physical Fibre Channel ports and 2 physical GbE ports.
- The Brocade 7800 switch has 16 physical Fibre Channel ports and six physical GbE ports.
- The FX8-24 blade has 12 physical Fibre Channel ports, 10 GbE ports, and two physical 10GbE ports.

FCIP configuration requirements for FICON extension

FICON extension uses FCIP for transport. FCIP interfaces and tunnels used for FICON extension must be defined prior to configuring FICON emulation. Ports should remain persistently disabled until after FICON emulation is configured. Refer to *Brocade FCIP Administrator's Guide* for information about configuring FCIP interfaces, tunnels, and circuits.

Configuration requirements for switches and directors

There are three configuration issues to consider when an extension switch or blade is connected to a switch in a FICON configuration:

- If you are creating a cascaded configuration (connecting two switches or directors with different domain IDs), be aware of IBM requirements for high integrity fabrics.
- In configurations with ISLs, ensure that ISL paths are properly configured to meet FICON emulation requirements for a determinate path for FICON commands and responses.
- When running FICON emulation features over an FCIP tunnel, it is highly recommended that both switches providing the FCIP tunnel are using the same Fabric OS release level.

High integrity fabric requirements for cascaded configurations

You can use extended FICON connections between or through Brocade 7800 Extension Switches or the FR4-18i or FX8-24 blade to create a cascaded FICON switched configuration. The fabric must be set up to provide a secure, or high integrity, fabric to enable this configuration to operate in an IBM environment. See Chapter 2, "Administering FICON Fabrics" for an explanation of these requirements.

FICON emulation requirement for a determinate path

FICON emulation processing creates FICON commands and responses on extended CHPIDs, and intercepts all exchanges between a channel and a CU. For FICON Emulation processing to function correctly, all the exchanges between a channel and CU must take a single tunnel path.

There are two ways to ensure a determinate path for FICON commands and responses:

- Define only one FCIP tunnel between sites.

- Use a Traffic Isolation zone (TI Zone) to assign a specific tunnel to Channel and control unit ports. In the cases where multiple tunnels are required between a pair of FICON switches (or Logical Switches), use TIZ to define ports that should use specific tunnels.

FCIP tunnel between sites

The Brocade 7800 and FX8-24 uses FCIP Trunking features to overcome the limitation of one Ethernet interface, one IP address and one FCIP tunnel. In Fabric OS v6.3 and later an FCIP Tunnel is created with multiple FCIP circuits over different IP interfaces to provide WAN load balancing and failover recovery in the event of a limited WAN outage. This provides a highly redundant WAN configuration for all FICON or FCP emulation technologies with Fabric OS. Figure 13 shows that a tunnel can have up to 4 circuits per GbE port.

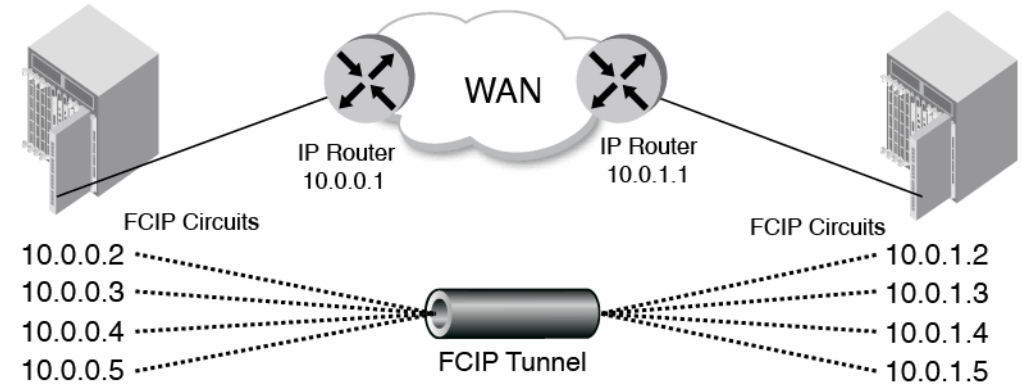


FIGURE 13 FCIP tunnel and circuits

Traffic Isolation Zoning

The Traffic Isolation Routing feature may be used to control the flow of interswitch traffic through the Brocade extension switch or blade VE_Port or E_Port connections. Traffic Isolation Routing uses a special zone, called a Traffic Isolation zone (TI zone), to create dedicated paths for specific traffic. For more information on Traffic Isolation Routing and creating zones, refer to the *Fabric OS Administrator's Guide*.

When setting up TI Zones in your FICON environment, it is not recommended to have failover enabled for the following reasons:

- FICON Emulation will not occur on a failed over path.
- FICON devices are identified at one time during channel path activation (ELP/LPE exchange) — if the paths do not fail, the MVS system will not re-issue this sequence over the recovery path.
- Multiple error periods will be perceived at the connected LPARs (first link failure, movement of traffic to recovery path and then again when the primary path is restored).
- There is no good way to perform a forced or controlled fallback.

Keep the following best practices in mind when using TI zoning:

- If TI Zones are used to provide routes for Emulated traffic then TI Zone Fail-over cannot be enabled.
- Keep the configurations as simple as possible, this will make the systems more supportable.
- Include virtual E_Ports in the Traffic Isolation zone.

- Use TI zoning for route selection on a port-to-port basis.
- Use port zoning to restrict data flows.
- Look at TI zoning, link costs, and zoning definitions to understand the routing paths used in your data center.
- Understand bandwidth requirements, available network resources, etc.
- Collect information on all new installations or after network changes by running the **portCmd --ipPerf** command.
- Separate disaster recovery networks from production networks.

Configuring FICON emulation

Before you configure FICON emulation, you need to understand the available options, and whether those options are to be implemented in your installation. If FICON emulation is new to you, read "FICON emulation overview" on page 43.

ATTENTION
Make sure both ends of the tunnel match before bringing it up or the tunnel will not form.

1. Verify that the following ports are opened in the IP network for FCIP:
   - TCP 3225—FC Class F frames
   - TCP 3226—FC Class 2 and 3 frames
   - TCP 3227—Brocade proprietary IP path performance utility (ipPerf)
   - IP protocol 6—Transmission Control Protocol
   - IP protocol 108—IP Payload Compression Protocol (IPComp)

   NOTE
   The 4 Gbps platform uses TCP port 3227 for ipPerf and IP protocol 108 for compression.

   The 8 Gbps platform runs over the FCIP tunnel, not TCP/IP directly like ipPerf. No specific TCP port is needed. Also the 8 Gbps platform compresses at layer 4 and no protocol is used.
2. Verify that the firmware is version v6.1.0e or later using the **firmwareShow** command.
3. Verify the correct licenses are installed using the **licenseShow** command. You can verify all slot-based licenses in a chassis using the **licenseslotcfg –show** command.
4. Verify the switches have been set up according to the instructions in "Configuring switched point-to-point FICON" on page 18 and "Configuring cascaded FICON" on page 21.
5. Configure the FCIP tunnel according to the *Brocade FCIP Administrator's Guide*.
6. Enable compression on the FCIP tunnel.
7. Configure FICON emulation on the tunnel that is solution-specific.
8. If you have more than one tunnel being configured, take the following actions:
   - If there is more then one tunnel to the same destination and their tunnel commit rates are different, configure the link cost values the same.
   - Configure TI Zones ensuring that if there are multiple E_Ports of different link costs, from one switch to another switch within TI Zones, configure the link cost values to be the same.

Configuring emulation on the FR4-18i blade

The following example shows FICON emulation on ge1 over tunnel ID 0 with FICON IBM z/OS Global Mirror emulation, tape write pipelining, tape read pipelining, TIN/TIR, and device level ACK emulation enabled. The default values are assumed for wrtMaxPipe, wrtMaxDev, wrtTimer, and wrtMaxChains. An oxidbase value of 0x7000 is specified.

```
switch:admin> portcfg ficon ge1 0 config -x 1 -w 1 -r 1 -t 1 -l 1 oxidbase 0x7000
```

Configuring emulation on the 7800 switch and FX8-24 blade

The following example shows FICON emulation for VE_Port 23 on a 7800 extension switch with Teradata read, Teradata write, printer emulation, tape write pipelining, tape read pipelining, TIN/TIR, and device level ACK emulation enabled. The default values are assumed for max-read-pipe, max-write-pipe, write-timer and write-chain. An oxidbase value of 0x7000 is specified.

Following are examples for enabling IBM z/OS Global Mirror emulation (formerly XRC emulation), Teradata emulation, and tape read and write pipelining.

```
portcfg fciptunnel 23 modify --ficon-xrc 1

portcfg fciptunnel 23 modify --ficon-tera-read 1 1 --ficon-tera-write 1

portcfg fciptunnel 23 modify --ficon-tape-write 1 --ficon-tape-read 1
```

Displaying FICON emulation configuration values

Display FICON emulation configuration values using examples in this section.

FR4-18i blade

For a Brocade FR4-18i blade, you can display the values configured for FICON emulation by using the portShow ficon command. The following example shows FICON emulation configuration values for port ge1.

```
switch:admin> portshow ficon ge1 all
Port: ge1
VE_STATUS
TunnelId vePort vePortStatus veFeatureBitMap veHashEntryCount
   0      24       UP              1              2
   1      ff     DOWN              0              0
   2      ff     DOWN              0              0
   3      ff     DOWN              0              0
   4      ff     DOWN              0              0
   5      ff     DOWN              0              0
   6      ff     DOWN              0              0
   7      ff     DOWN              0              0
FEATURES
TunnelId XRC TapeWrt  TapeRd  TinTir  DvcLack  RdBlkId
   0       ON     ON       ON      ON      ON       OFF
   1      OFF    OFF      OFF     OFF     OFF       OFF
   2      OFF    OFF      OFF     OFF     OFF       OFF
   3      OFF    OFF      OFF     OFF     OFF       OFF
   4      OFF    OFF      OFF     OFF     OFF       OFF
```

```
   5      OFF    OFF      OFF     OFF     OFF       OFF
   6      OFF    OFF      OFF     OFF     OFF       OFF
   7      OFF    OFF      OFF     OFF     OFF       OFF
PARAMETERS
TunnelId WrtPipe RdPipe WrtDevs RdDevs WrtTimer WrtChain OxidBase DebugFlags
   0      032     032     16      16     0300    3000000  0x7000  0xffc80000
   1      000     000     00      00     0000    0000000  0x0000  0x00000000
   2      000     000     00      00     0000    0000000  0x0000  0x00000000
   3      000     000     00      00     0000    0000000  0x0000  0x00000000
   4      000     000     00      00     0000    0000000  0x0000  0x00000000
   5      000     000     00      00     0000    0000000  0x0000  0x00000000
   6      000     000     00      00     0000    0000000  0x0000  0x00000000
   7      000     000     00      00     0000    0000000  0x0000  0x00000000
```

7800 switch and FX8-24 blade

For a Brocade 7800 and FX8-24 blade, use the **portShow fciptunnel** command to determine the FICON emulation settings. The following example show the FICON emulation settings for VE_Port 16.

```
portshow fciptunnel 23
----------------------------------------
Tunnel ID: 23
   Tunnel Description:
   Admin Status: Enabled
   Oper Status: Up
   Compression: On (Aggressive)
   Fastwrite: Off
   Tape Acceleration: Off
   TPerf Option: Off
   IPSec: Disabled
   QoS Percentages: High 50%, Med 30%, Low 20%
   Remote WWN: Not Configured
   Local WWN: 10:00:00:05:1e:55:6a:45
   Peer WWN: 10:00:00:05:1e:55:66:45
   Circuit Count: 4
   Flags: 0x00000000
   FICON: On
      FICON XRC: On
      FICON Tape Write: On
      FICON Tape Read: On
      FICON TinTir Emul: On
      FICON Dvc Acking: On
      FICON Read BLK-ID: Off
      FICON Teradata Write: On
      FICON Teradata Read: On
      Tape Write Pipe: 32
      Tape Read Pipe: 32
      Tape Write Devs: 16
      Tape Read Devs: 16
      Tape Write Timer: 300
      Tape Max Chain: 3200000
      FICON OXID Base: 0x8000
      FICON Debug Flags: 0xf7898030
```

Modifying FICON emulation

FICON emulation may be enabled on a per FCIP tunnel basis. For the FR4-18i blade, use the **portCfg ficon modify** command to make modifications to the feature. For the Brocade 7800 switch and FX8-24 blade, use the **portCfg fciptunnel** command.

For details on command usage, refer to the *Fabric OS Command Reference*.

CAUTION

You will need to bring the FCIP tunnel down in order to make changes. This process is disruptive to all traffic on the tunnel.

1. Connect to the switches at both ends of the FCIP tunnel and log in using an account assigned to the admin role.
2. Disable the FCIP tunnel at both ends where the FICON emulation feature is enabled.
3. Use the command appropriate for your switch or blade model:
   - For the Brocade FR4-18i, use the **portCfg ficon modify** command.
   - For the Brocade 7800 switch or FX8-24, use the **portCfg fciptunnel modify** command.
4. Make matching FICON emulation changes to both ends of the tunnel.
5. Enable the FCIP tunnel.

Displaying FICON emulation performance statistics

You can use the **portShow** command to view the performance statistics and monitor the behavior of FICON emulation. You do not need to disable any feature to display statistics.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **portShow ficon** command to display the statistics for the FR4-18i blade. Enter **portShow extun** command to display statistics for the 7800 switch or FX8-24 blade.

   Refer to the *Fabric OS Command Reference* for more information on the variables you can use to display the various FICON statistics.

FICON emulation monitoring

Use examples in this section to display emulation monitoring for extension blades and switches.

Use the **-emul** argument for the **portShow ficon** and **portShow xtun** command to monitor FICON emulation. Following are examples of these commands:

- Following is an example for the FR4-18i blade.

  ```
  switch:admin> portshow ficon [slot/}ge_port tunnelId -ficon -emul
  ```

- Following is an example for the 7800 switch or FX8-24 blade.

  ```
  switch:admin> portshow xtun [slot/}ve_port -ficon -emul
  ```

Following is a tape output example for FR4-18i blade. Output for the 7800 switch and FX8-24 blade is similar.

```
TAPE EMULATION STATS
+----------+----------------+-+-----+----+----+----+-----------+----------+------+----------+----+
| FDCB Ptr |     Path       |H|State|Emul|Emul|Rtry| Emulated  |Emulated  |RdAvg |Emulated  |WtAvg |
|  (0x)    |     (0x)       |D|     |Pipe|Q'd | Qd | Tape Ops  |Read CCWs | Size |Write CCWs| Size |
+----------+----------------+-+-----+----+----+----+-----------+----------+------+----------+----+
|0x10018A00|2463016406050000|H| 0x14|0x20|000E|0000|      13212|         0|     0|    125754| 32760|
|0x1001E800|2463016406050001|H| 0x14|0x20|001A|0000|      13647|         0|     0|    128776| 32760|
|0x1001C400|2463016406050002|H| 0x18|0x20|000A|0000|      13164|         0|     0|    125758| 32760|
|0x1001CC00|2463016406050003|H| 0x14|0x20|0008|0000|      13908|         0|     0|    131716| 32760|
|0x1002BC00|2463016407050000|H| 0x14|0x20|0008|0000|      10094|         0|     0|     97917| 32760|
|0x10027B00|2463016407050001|H| 0x14|0x20|0011|0000|       8915|         0|     0|     85966| 32760|
|0x1002C400|2463016407050002|H| 0x14|0x20|0007|0000|      10365|         0|     0|     99742| 32760|
|0x1002B000|2463016407050003|H| 0x14|0x20|0008|0000|       9993|         0|     0|     96088| 32760|
|0x1003F000|2463046401050100|H| 0x00| N/A|0000|0000|      19392|         0|     0|    183111| 32760|
|0x1003E400|2463046401050101|H| 0x00| N/A|0000|0000|      19342|         0|     0|    183111| 32760|
|0x10041800|2463046401050102|H| 0x00| N/A|0000|0000|      19420|         0|     0|    183111| 32760|
|0x10040400|2463046401050103|H| 0x00| N/A|0000|0000|      19450|         0|     0|    183111| 32760|
|0x10049800|2463046402050100|H| 0x00| N/A|0000|0000|      19392|         0|     0|    183111| 32760|
|0x10045400|2463046402050101|H| 0x00| N/A|0000|0000|      19436|         0|     0|    183111| 32760|
|0x10045000|2463046402050102|H| 0x00| N/A|0000|0000|      19456|         0|     0|    183111| 32760|
|0x10048000|2463046402050103|H| 0x00| N/A|0000|0000|      19404|         0|     0|    183111| 32760|
+----------+----------------+-+-----+----+----+----+-----------+----------+------+----------+----+
```

XRC output example:

```
                              XRC EMULATION STATS
+----------+----------------+-+-----+----+----+----+----+-----------+---+------+------+
| FDCB Ptr |     Path       |H|State|Cmds| Cmd|Data|Data| Emulated  |Avg|   RRS|  RRS |
|  (0x)    |     (0x)       |D|     | Qd | Max| Qd |Max | RRS Ops   |RRS|   TLF|  Read|
+----------+----------------+-+-----+----+----+----+----+-----------+---+------+------+
|0x1017DC00|24B100B20E11092B|H| 0x00|0000|000F|0000|0230|      47184|213| 25636| 16063|
|0x104B4C00|24B100B20E1109F7|H| 0x00|0000|000F|0000|01E0|       3961|146| 41409| 26313|
|0x104B5000|24B100B20E1109F8|H| 0x00|0000|000F|0000|1112|       3855|148| 41613| 27182|
|0x104B5800|24B100B20E1109F9|H| 0x00|0000|000F|0000|1493|       4365|153| 36604| 20090|
|0x104B6000|24B100B20E1109FD|H| 0x00|0000|000F|0000|1422|       3983|144| 40358| 24305|
|0x103B7C00|24B102B20F11092B|H| 0x00|0000|000F|0000|0F52|      46658|212| 25910| 16283|
|0x104B4400|24B102B20F1109F7|H| 0x00|0000|000F|0000|0C42|       4159|147| 39379| 23225|
|0x104B4800|24B102B20F1109F8|H| 0x00|0000|000F|0000|1112|       4038|147| 41523| 26894|
|0x104B5400|24B102B20F1109F9|H| 0x00|0000|000F|0000|05E8|       4185|155| 38116| 22943|
|0x104B5C00|24B102B20F1109FD|H| 0x00|0000|000F|0000|07E2|       3755|143| 40929| 24885|
+----------+----------------+-+-----+----+----+----+----+-----------+---+------+------+
```

IBM z/OS Global Mirror emulation (formerly eXtended Remote Copy or XRC) and Tape statistics are presented differently in output formats. The following elements are common to both Tape Emulation and IBM z/OS Global Mirror Emulation outputs:

FDCB ptr — A pointer to the FICON Device Control Block. Support personnel may use this pointer.

Path — The device path, in the format VE-HD-HP-DD-DP-LP-CU-DV. where:

- VE is the internal VE_Port number.
- HD is the hex value for the Host Domain (the entry domain for this host port into the fabric).
- HP is the hex value for the Host Port (the entry port of this host connection into the fabric).
- DD is the hex value for the Device Domain (the entry domain for this device into the fabric).
- DP is the hex value for the Device Port (the entry port for this device connection into the fabric).
- LP is the Logical Partition (LPAR) value for the host accessing the specific device.
- CU is the Control Unit number (CUADDR) for the specific FICON connection.
- DV is the Device Number of this FICON connected device.

For example, the value 2463016406050001 breaks down as follows.

VE	HD	HP	DD	DP	LP	CU	DV
24	63	01	64	06	05	00	01

State — A value of zero indicates emulation is idle. Any non-zero value indicates emulation is active.

FICON emulation statistics

Use the **portShow xtun <slot/>ve_port -ficon -stats [options]** command to view statistics and monitor the behavior of FICON emulation on 7800 switches and FX8-24 blades. You can use the following options for the three performance monitors for the emulation features: -**teraperf**, -**xrcperf**, and -**tapeperf**. Refer to the *Brocade Fabric OS Command Reference Manual* for more information.

General statistics

Use **portshow xtun [slot\}ve_port -ficon -stats** to display general FICON emulation (including Teradata, XRC, and tape emulation) statistics on 7800 switches and FX8-24 blades.

```
FICON FCIP Tunnel=0 Statistics:
 Emulation Common Statistical Counts (decimal)
 =============================================
 TotalIngressFrames    =             25147833
 TotalEgressFrames     =             42506209
 TotalFCEgressFrames   =              3636219
 TotalCmds             =              1817668
 TotalEmulDvcLvlAcks   =                   54
 TotalEmulatedOps      =              1815454
```

```
 MaxRetryQueueDepth    =          0   MaxEgressQueueDepth  =        224
 TotalCUBusyResponses  =          0   TotalCUEndResponses  =          0
 TotalEmulatedCUBusys  =          0   TotalEmulCUEnd       =          0
 TotalSelectiveResets  =         16   TotalChLinkBusy      =          7
 TotalCancels          =          1   TotalAborts          =          1
 TotalEmulErrors       =          0   TotalCuLinkBusy      =          0
 TotalPurgePaths       =          0   Xport LRC CheckErrors=          0
 Generated Link Busys  =          0   Failed Generate Frame=          0

 WIRE Buffer Percentages LocalFree= 95 LocalLow= 95 PeerFree= 95 PeerLow=95
 XBAR Buffer Percentages LocalFree= 98 LocalLow= 98 PeerFree= 98 PeerLow=98

 FICON Configuration Status:
 -------------------------------------------------------------------
  FICON Host side Paths =       2 Device Side Paths=   0
  FICON LPARS Connected =       6    Curr LCUs =      10 Total Devices=  25
  Current Egress Q Count=      52    RetryQCnt =       0
  Current Free Headers  =      63    HdrsInUse =       0
  Active Emulation Count= 2

XRC Emulation Statistical Counts (decimal)
 ------------------------------------------------------------
 Total XRC Overlapped Exchange count =                  344
 Total Emulated RRS Chains           =              9440151
 Total Emulated RRS Commands         =              9440151
 Total Received RRS Bytes            =            377606040
 Total XRC RRS Requests in Bytes     =         555685048464
 Average RRS Request BlkSize         =                   40
 Average RRS Requests per Chain      =                    1
 Largest RRS Request Byte Count      =                58864
 Ratio of RRS Read Bytes to the
 Requested Read bytes = 0 read : 1000 requested

Tape Write Emulation Statistical Counts (decimal)
 ------------------------------------------------------------
  Current Bytes in write pipe         =              1015560
  Maximum Bytes in write pipe         =             26864400
  Largest write chain processed       =              4128769
  Total number of emulated Write Bytes=       14053917200357
  Number of emulated Write Chains     =            103735831
  Total number of emulated Write CCWs =            376828157
  Average Emulated Writes Blocksize   =                37295
  Average Writes in Emulated Chains   =                    3
  Write emulation slowdowns           =              3233062
  Slowdowns at Start of Chain         =              1672232
  Slowdowns at End of chain           =              1560830
  Current Host side Write FDCB Count  =                   16
  Max Concurrent Write FDCB Count     =                   24
  Current Write Limited FDCB Count    =                   16

 Tape Read Emulation Statistical Counts (decimal)
 -------------------------------------------------
  Total number of emulated Read Bytes =       13624542616969
  Total number of emulated Read Chains=             96462808
  Total number of emulated Read CCWs  =            352663119
  Average Emulated Bytes per chain    =               141241
  Average Emulated Read Blocksize     =                38633
  Average CCWs in Emulated Chains     =                    3
  Current Read FDCBs Count            =                    8
  Max Concurrent Read FDCB Count      =                   24
```

```
 Current Read Limited FDCB Count     =                    0

Tera Write Emulation Statistical Counts (decimal)
------------------------------------------------------------
 Current Bytes in write pipe         =                    0
 Maximum Bytes in write pipe         =              1405952
 Largest write chain processed       =                43936
 Total number of emulated Write Bytes=          19204226768
 Number of emulated Write Chains     =               989882
 Total number of emulated Write CCWs =               989882
 Average Emulated Writes Blocksize   =                19400
 Average Writes in Emulated Chains   =                    1
 Write emulation slowdowns           =                  114
 Slowdowns at Start of Chain         =                    0
 Slowdowns at End of chain           =                  114
 Single Chain Emulation Counter      =                    0
 Write Paced Count                   =                    0
 Current Host side Write FDCB Count  =                    1
 Max Concurrent Write FDCB Count     =                    1
 Current Write Limited FDCB Count    =                    0

Tera Read Emulation Statistical Counts (decimal)
-------------------------------------------------
 Total number of emulated Read Bytes =          17688908128
 Total number of emulated Read Chains=               825572
 Total number of emulated Read CCWs  =               825572
 Average Emulated Bytes per chain    =                21426
 Average Emulated Read Blocksize     =                21426
 Average CCWs in Emulated Chains     =                    1
 Read Block Paced Count              =                    0
 Read Not Ready Situations Count     =                    0
 Current Read FDCBs Count            =                    1
 Max Concurrent Read FDCB Count      =                    1
 Current Read Limited FDCB Count     =                    1

FICON Debug Flags (ftrace and others) = 0xf7c90000 (Default = 0xf7c90000)
-----------------------------------------------------
 Bit 31 [0x80000000] = 1 : TRIGGER_ON_SELRESET
 Bit 30 [0x40000000] = 1 : TRIGGER_ON_PURGEPATH
 Bit 29 [0x20000000] = 1 : TRIGGER_ON_RRS_MISS
 Bit 28 [0x10000000] = 1 : TRIGGER_ON_LRJ

 Bit 27 [0x08000000] = 0 : TRIGGER_ON_UNIT_CHECK
 Bit 26 [0x04000000] = 1 : TRIGGER_ON_LOOKUP_FAIL
 Bit 25 [0x02000000] = 1 : TRIGGER_ON_FDCB_ABORT
 Bit 24 [0x01000000] = 1 : TRIGGER_ON_NOFDCB_ABORT

 Bit 23 [0x00800000] = 1 : TRIGGER_ON_LINKDOWN
 Bit 22 [0x00400000] = 1 : TRIGGER_ON_SENSE_CMD
 Bit 21 [0x00200000] = 0 : TRIGGER_ON_BUSYATTN
 Bit 20 [0x00100000] = 0 : TRIGGER_ON_XRCUNS

 Bit 19 [0x00080000] = 1 : DISPLAY_FDCB_ON_ERROR
 Bit 18 [0x00040000] = 0 : TRIGGER_ON_LOW_WIREPOOL
 Bit 17 [0x00020000] = 0 : TRIGGER_ON_READ_UNITCHECK
 Bit 16 [0x00010000] = 1 : TRIGGER_ON_STATE_SAVE

 Bit 15 [0x00008000] = 0 : TRIGGER_ON_SUSPEND
 Bit  4 [0x00000010] = 0 : ACCEPT_READTRACK_STATUS
```

```
 Bit  3 [0x00000008] = 0 : FORCE_DISABLE_READ_PIPE
 Bit  2 [0x00000004] = 0 : FORCE_DISABLE_WRITE_PIPE
 Bit  1 [0x00000002] = 0 : FORCE_DISABLE_XRC_EMUL
 Bit  0 [0x00000001] = 0 : DISABLE_PERSIST_IU_PACE
```

Teradata emulation performance statistics

Use **portshow xtun <veport> -ficon -teraperf** to display Teradata performance statistics on 7800 switches and FX8-24 blades as in the following example.

```
Tera Performance Monitor Data:
==============================
    Sample Time Period in ms: 4318

 Tera Write Performance Data:
 ---------------------------
     Emulated Chains per sec: 1186
       Emulated CCWs per sec: 1186
        Ave Write Block Size: 22617
          Emulated Write BPS: 26831514

 Tera Read Performance Data:
 ---------------------------
     Emulated Chains per sec: 1069
       Emulated CCWs per sec: 1069
         Ave Read Block Size: 10780
           Emulated Read BPS: 11531104
```

FICON tape emulation performance statistics

Use **portshow xtun <veport> -ficon -tapeperf** to display FICON tape pipelining performance statistics. on 7800 switches and FX8-24 blades as in the following example.

```
Tape Performance Monitor Data:
==============================
    Sample Time Period in ms: 9794
 Tape Write Performance Data:
 ---------------------------
     Emulated Chains per sec: 133
       Emulated CCWs per sec: 1085
        Ave Write Block Size: 32760
          Emulated Write BPS: 35558640
 Tape Read Performance Data:
 ---------------------------
     Emulated Chains per sec: 38
       Emulated CCWs per sec: 318
         Ave Read Block Size: 32760
           Emulated Read BPS: 10431720
```

FICON XRC emulation performance statistics

Use **portshow xtun <veport> -ficon -xrcperf** to display XRC (also known as IBM z/OS Global Mirror) performance statistics on 7800 switches and FX8-24 blades as in the following example.

```
XRC Performance Monitor Data:
=============================
    Sample Time Period in ms: 12874
     Emulated Chains per sec: 250
   Emulated RRS Cmds per sec: 35000
  Emulated RRS Bytes per sec: 140000000
     Average RRS Update Size: 4000
```

Chapter

Maintaining and Troubleshooting FICON 5

In this chapter

- Firmware management in a FICON environment 61
- Configuration restoration in a FICON environment 62
- Traffic Isolation Zoning 63
- Port fencing 70
- FICON information 71
- Port swapping 74
- Blade swapping 75
- Common FICON issues 76
- Troubleshooting FICON 79
- Troubleshooting FICON CUP 81
- Troubleshooting NPIV 82

Firmware management in a FICON environment

You can use either the CLI or Brocade Network Advisor (BNA) to upgrade or downgrade your Fabric OS. Go to http://www.brocade.com and follow the link “Brocade Connect Login” to access firmware packages. Registered users can log in and follow the links for downloads. New users can easily register and download release notes.

Firmware is downloaded in a .gz or .zip file. The Brocade Network Advisor has intelligence built-in that unbundles the necessary files, making it unnecessary to unbundle the package. With both Web Tools or the CLI, it will be necessary to unzip or ungunzip the package first.

For more information on the firmware download process, refer to the *Fabric OS Administrator’s Guide*.

Upgrade and downgrade considerations

Concurrent upgrades are generally supported from one major release level to the next, for example, v6.4.x to v7.x. As a precaution, always read the appropriate section in the Brocade Fabric OS Release Notes before upgrading or downgrading firmware.

NOTE
Firmware may need to be upgraded in multiple steps. Consult the Release Notes for details.

When downgrading firmware, turn off and disable all features not supported in the final release. For more information on the firmware download process, refer to the *Fabric OS Administrator’s Guide*.

Firmware upgrade disruption

Loading new firmware is a non-disruptive process except for the following:

- During the firmware download process a failover to the backup processor occurs. Any outstanding CUP commands are lost and result in a timeout. To avoid this, CUP should be varied offline before starting a firmware download. The CUP may be varied back online after a successful firmware download.
- All firmware downloads will cause an I/O disruption when the new code is activated on the FX8-24 blade and 7800 switch.

NOTE
If upgrading multiple switches or blades, upgrade one at a time. This is not a requirement for DCX or DCX-4S platforms.

Non-disruptive firmware upload and download

All systems maintain two partitions of nonvolatile storage areas, a primary and a secondary. Following is an overview of the firmware download process:

1. The firmware is downloaded to the secondary partition.
2. The current secondary and primary partitions are swapped.
3. The CP then reboots. In dual CP systems (Brocade 48000 and Brocade DCX enterprise-class platforms) the backup CP is rebooted with the new firmware and the HA failover is automatically invoked.
4. Once rebooted, the primary code image is copied to the secondary.

Configuration restoration in a FICON environment

If the switch is operating in a FICON CUP environment, and the ASM (Active=Saved) bit is set on, then the switch ignores the IPL file downloaded when you restore a configuration. Table 5 describes this behavior in more detail.

TABLE 5 Backup and restore in a FICON CUP environment

ASM bit	Command	Description
on or off	configUpload	All the files saved in the file access facility are uploaded to the management workstation. A section in the uploaded configuration file labeled FICON_CUP is in an encoded format.

TABLE 5 Backup and restore in a FICON CUP environment (Continued)

ASM bit	Command	Description
on	configDownload	Files saved on the switch that are also present in the FICON_CUP section of the configuration file are overwritten. Files in the FICON section of the configuration file that are not currently present on the switch are saved. The IPL file is replaced, because active=saved mode is on. A warning message is displayed in the syslog to warn that the IPL file is not being overwritten.
off	configDownload	Files saved on the switch that are also present in the FICON_CUP section of the configuration file are overwritten. Files in the FICON section of the configuration file that are not currently present on the switch are saved. The IPL file is not replaced, because active=saved mode is off.

If *fmsmode* is enabled in a configuration file, but is disabled on the switch, the **configDownload** command fails and displays an error message. This prevents undesirable conditions that could result from enabling *fmsmode* on a switch that does not require it.

Traffic Isolation Zoning

Traffic Isolation (TI) Zoning allows data paths to be specified. In a FICON fabric you need Fabric OS v6.2.0 or later. TI Zoning has the following benefits:

- Separates direct attached storage device (DASD) and tape traffic.
- Selects traffic for diverse ISL routes (typical of dual fiber networks).
- In conjunction with long-distance channel extension equipment (FICON Acceleration), guarantee bandwidth for certain mission-critical data.

For more information on Traffic Isolation Zoning, refer to the *Fabric OS Administrator's Guide*.

Determining ports for the TI Zone

To find the device ports, use the MVS display command. The following example shows how to determine where device D000 is connected and the paths to it, from the MVS console enter:

```
D M=DEV (D000)
Response is:
DEVICE D000 STATUS=ONLINE
CHP 9C 9D 9E 9F
ENTRY LINK ADDRESS 883C 883D 883E 883F
DEST LINK ADDRESS 790C 790D 790E 790F
PATH ONLINE Y Y Y Y
CHP PHYSICALLY ONLINE Y Y Y Y
PATH OPERATIONAL Y Y Y Y
MANAGED N N N N
CU NUMBER D000 D000 D000 D000
MAXIMUM MANAGED CHPID(S) ALLOWED: 0
DESTINATION CU LOGICAL ADDRESS = 10
SCP CU ND = 002107.921.IBM.07.000000002036.0086
SCP TOKEN NED = 002107.900.IBM.07.000000002036.1000
SCP DEVICE NED = 002107.900.IBM.07.000000002036.1000
```

Enhanced TI Zoning

Enhanced Traffic Isolation Zones allow you to specify a preferred and exclusive path through a cascaded fabric for a particular flow by defining a set of devices or ports to appear in more than one Enhanced TI Zone. A preferred path is one that has *failover enabled* and an exclusive path has *failover disabled*. An exclusive path in the following topologies is beneficial as it will limit the number of hops between directors:

- Triangular
- System Data Mover
- Emulation

Enhanced TI Zoning for the topologies listed above is available only on the following platforms running Fabric OS v6.4.0 or later:

- Brocade 5100
- Brocade 5300
- Brocade 7800
- Brocade DCX
- Brocade DCX-4S

Triangular topology

The triangular topology shown in Figure 14 is a common FICON deployment for managing data center recovery functions. In this topology, a director is located in each of three sites and connected to the other two forming a triangle. In most environments, the purpose of this configuration is to give the host application the ability to connect to storage media at the other two sites, which allow it to recover from an outage at either site. Meanwhile, the storage systems constantly synchronize between the two storage sites.

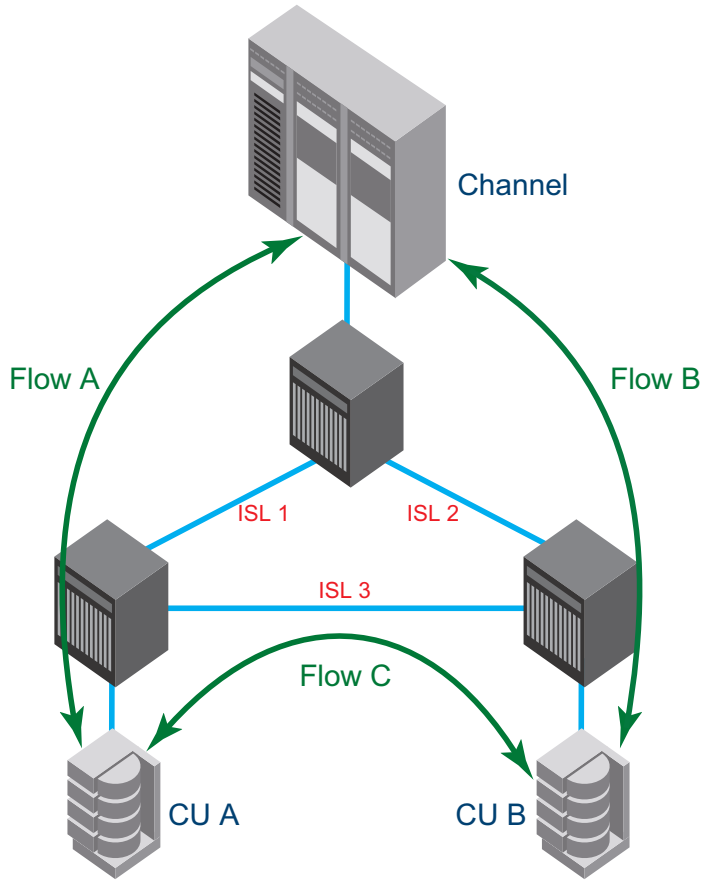


FIGURE 14 Typical triangular setup

During normal operation, the routes from any device on one director are a one-hop path to either of the other two directors. However, if the path between any pair of directors fails then a two-hop path is available. Multi-hop paths are not certified for FICON configurations.

To get around the multiple-hop issue, use Enhanced TI Zoning to prohibit the connection between E_Ports on the directors. For this setup you must define a device in two zones with failover disabled. Figure 15 shows that the setup allows a source device to reach two separate destinations over exclusive, one-hop paths, while preventing the source device from taking the two-hop path in the event of a failure.

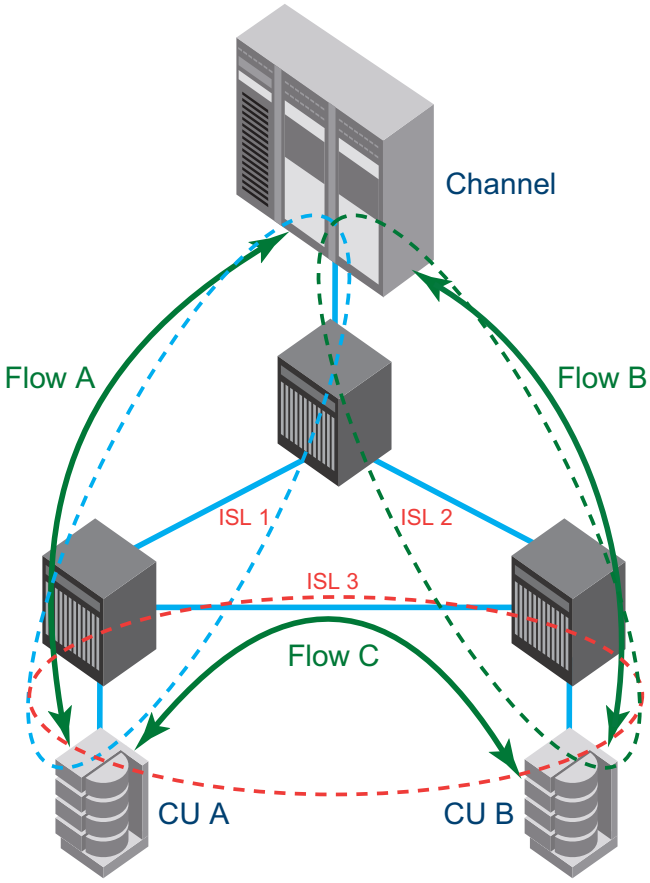


FIGURE 15 Triangular topology with Enhanced TI Zones

Figure 15 shows the following TI Zone definitions for the triangular topology:

- Blue Zone includes the channel, ISL 1, and CU A.
- Green Zone includes the channel, ISL 2, and CU B.
- Red Zone includes the CU A, ISL 3, and CU B.

Using these definitions with failover disabled, the topology achieves the desired behavior. The channel can reach CU A only over ISL 1 and CU B only over ISL 2. If either ISL should fail, connectivity to the destination with the failed ISL is prevented because the exclusive path has failed.

System Data Mover topology

Figure 16 shows a cascaded topology which can be used to support an operations recovery site. In this environment, host and storage systems exist at both sites, which are connected by two directors cascaded together using the System Data Mover (SDM) application. The storage differs between the sites. In the production site, the storage is DASD to support fast access for production applications. In the backup site, the storage is tape to support archival operations for system restoration.

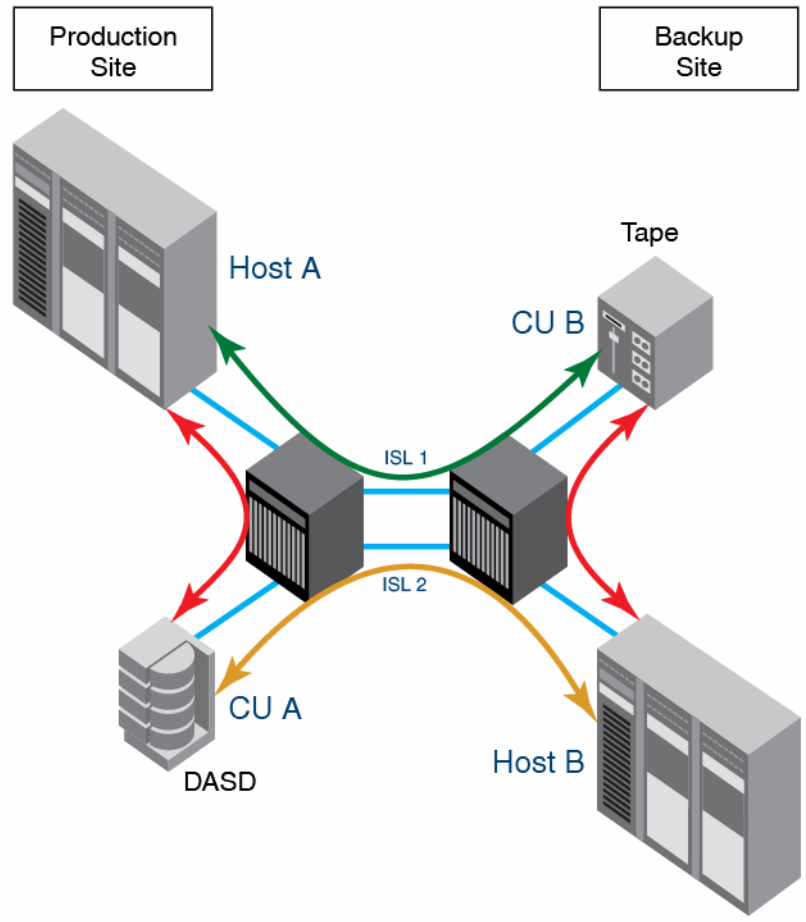


FIGURE 16 **Typical System Data Mover topology**

The host in the production site operates the SDM application that reads data from the DASD and writes it to the remote tape. The path to the remote site is required to be isolated to support the bandwidth requirements needed to write the data to the remote tape. The host in the backup site needs access to the DASD in the production site to support a hot recovery scenario in the event the production host goes down. Supporting these two functions requires the ability to define overlapping zones that isolate the tape traffic from the DASD traffic and allow local access to the DASD ports.

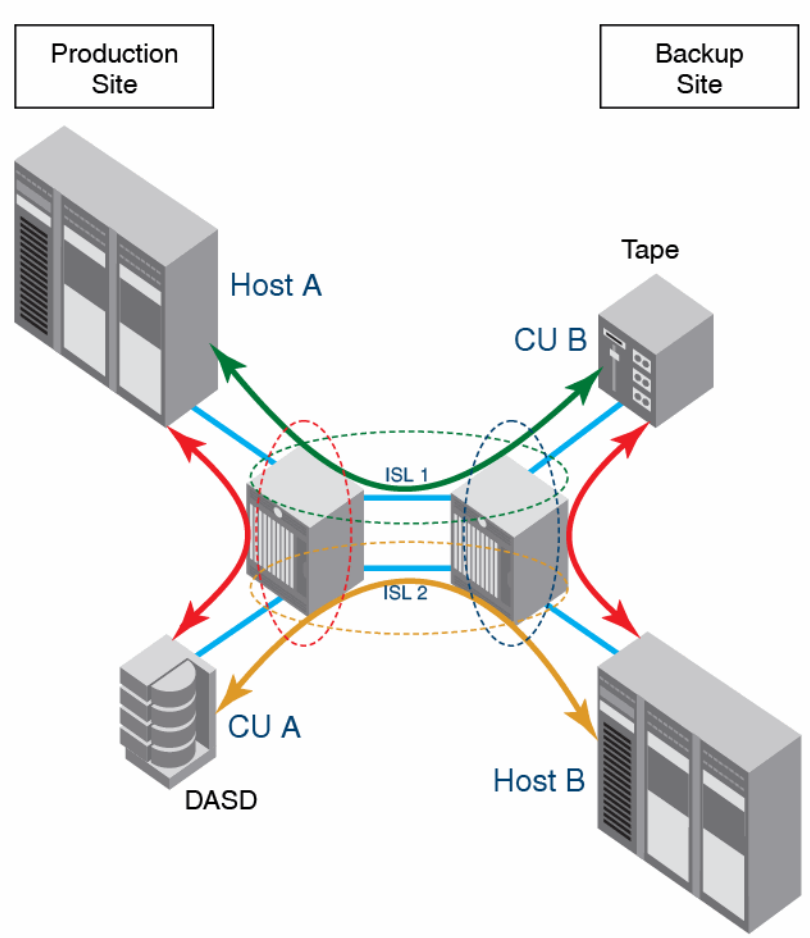


FIGURE 17 System Data Mover topology using Enhanced TI Zones

Figure 17 on page 68 shows the following Enhanced TI Zones definitions for the System Data Mover topology:

- Green Zone includes Host A, ISL 1, and CU B.
- Orange Zone includes CU A, ISL 2, and Host B.
- Red Zone includes Host A and CU A.
- Blue Zone includes Host B and CU B.

Using these definitions with failover disabled achieves the desired behavior. The production channels can access the local DASD and use an exclusive path to write data to the remote tape. The remote channels can access the remote tape and use an exclusive path to write data to the production DASD. In both cases, the production tape traffic is excluded from intruding on the backup DASD traffic and vice-versa.

Emulation topology

FICON device emulation topologies have unique requirements due to the characteristics of the emulation devices. Each device must track the emulated sessions and maintain the state of the emulated devices in order to satisfy both ends of the connection. Since this is done over very long distances, care must be taken when configuring the ISL connections to insure that the sessions remain along exclusive paths. By maintaining an exclusive path between the emulation units, the recovery scenarios become manageable and allow system level mechanisms to take precedence, that is the device level recovery at the channel or control unit.

Generally, channel to control unit access is deployed as one-to-many topology; where, one channel is defined to access many control units. FICON environments, however, are deployed in multiple redundant configurations that also define access from one control unit to many channels. When emulation is involved these configurations can result in overlapping channel and control unit connections that make emulation isolation difficult. By using the Enhanced TI Zoning feature to support device membership in multiple zones, these types of emulation configurations are addressed.

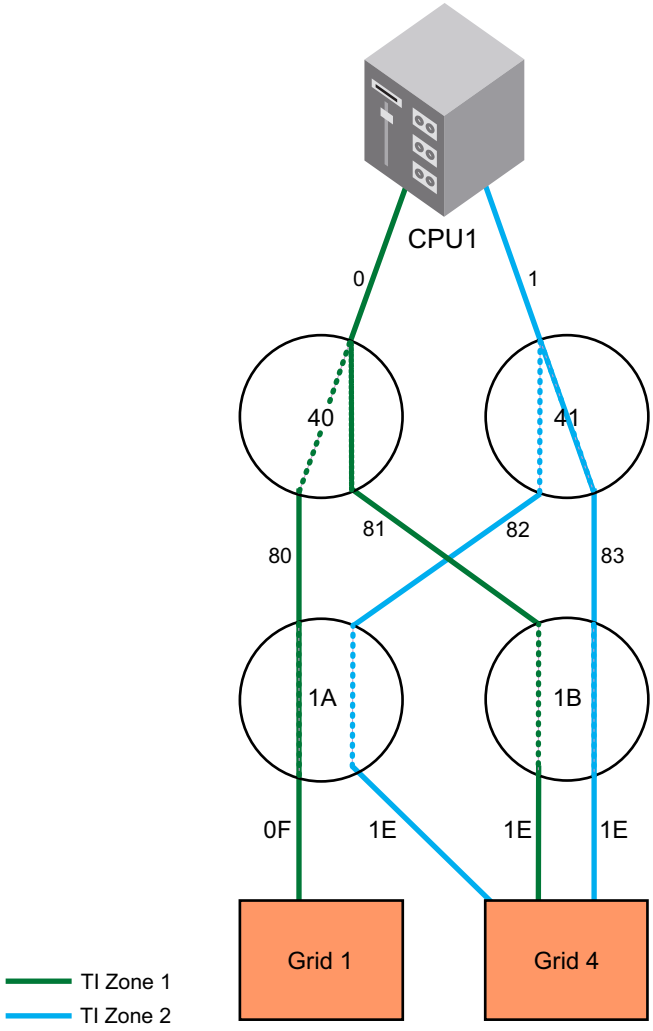


FIGURE 18 Emulation topology using Enhanced TI Zones

Figure 18 on page 69 shows the following Enhanced TI Zoning definitions for the emulation topology:

- Green TI Zone includes channel 0, ISL 80, ISL 81, Grid 1, and Grid 4.
- Blue TI Zone includes channel 1, ISL 82, ISL 83, and CU Grid-4.

The unique characteristic of these zones is that each channel is defined with two control unit device ports and one of the control unit device ports, CU Grid-4, is in both zones. In a traditional TI Zone definition, these zones would have to be combined to provide the appropriate connectivity, but then in the event of an ISL failure it would lead to a multi-hop, multi-emulation path that would severely affect performance. Multi-hop paths are not certified for FICON configurations.

Port fencing

Occasionally, bad optics and cables can cause errors to occur at a rapid rate that error processing and sending and processing RSCNs can cause fabric performance problems. Port fencing allows the user to limit the number of errors a port can receive by forcing a port offline when certain error thresholds are met.

The port fencing feature is configured through Fabric Watch. For more information on configuring Port Fencing, refer to the *Fabric Watch Administrator's Guide*.

Defining port fencing

1. (Optional) Clear all alarms.
2. Define threshold levels.
3. Define alarm action.
4. Activate alarming.

NOTE
Establish a Telnet session with a tool such as Putty that allows the columns to be increased. This is because some of the displays use more than the standard 80 columns that programs such as HyperTerminal support. Recommended number of columns is 120.

Settings for FICON environments

For typical FICON environments, port fencing is usually only set for CRC errors and Invalid Words. The default of 1,000 errors per minute is a little high for CRC errors and Invalid Words. A more common setting is 50 errors per minute. This is high enough to ignore occasional errors and transient errors due to re-cabling but low enough to stop problematic optics from causing fabric issues.

By default, the alarms are set to fence the port, log an alert, send an e-mail, and set an SNMP trap. In most FICON environments, only fencing the port and logging the alert are desired.

The following are the default thresholds:

- Low 0
- High 1,000 errors per minute

FICON information

You can display link incidents, registered listeners, node identification data, and FRU failures, as described in the following sections.

Link incidents

The registered link incident record (RLIR) ELS contains the link incident information sent to a listener N_Port.

To display link incidents, connect to the switch, log in as user, and enter one of the following commands:

- For the local switch: **ficonShow rlir**
- For all switches defined in the fabric: **ficonShow rlir fabric**

Identifying ports

The **ficonShow rlir** command displays, among other information, a tag field for the switch port. You can use this tag to identify the port on which a FICON link incident occurred. The tag field is a concatenation of the switch domain ID and port number, in hexadecimal format. The following example shows a link incident for the switch port at domain ID 120, port 93 (785d in hex):

```
switch:admin> ficonshow rlir
{
 {Fmt  Type PID    Port   Incident Count  TS Format   Time Stamp
  0x18 F    785d00   93               1  Time server Thu Apr 22 09:13:32 2004
  Port Status:          Link not operational
  Link Failure Type:    Loss of signal or synchronization

  Registered Port WWN     Registered Node WWN      Flag  Node Parameters
  50:05:07:64:01:40:16:03 50:05:07:64:00:c1:69:ca  0x10  0x200115
  Type number:          002064
  Model number:         103
  Manufacturer:         IBM
  Plant of Manufacture: 02
  Sequence Number:      0000000169CA
  tag:                  155d

  Switch Port WWN         Switch Node WWN          Flag  Node Parameters
  20:5d:00:60:69:80:45:7c 10:00:00:60:69:80:45:7c  0x00  0x200a5d
  Type number:          SLKWRM
  Model number:         24K
  Manufacturer:         BRD
  Plant of Manufacture: CA
  Sequence Number:      000000000078
  tag:                  785d
 }
}
The Local RLIR database has 1 entry.
```

Registered listeners

To display registered listeners for link incidents, connect to the switch, log in as user, and enter one of the following commands:

- For the local switch: **ficonShow lirr**
- For all switches defined in the fabric: **ficonShow lirr fabric**

Example of LIRR output:

```
switch_4:FID4:admin> ficonshow lirr
{Fmt  Type PID    Listener Port WWN       Switch Port WWN         Listener Type
 0x18 N    c10100 50:05:07:64:01:ff:ff:01 20:01:00:05:1e:57:da:5b Conditional-C*
 0x18 N    c10200 50:05:07:64:01:ff:ff:02 20:02:00:05:1e:57:da:5b Conditional-S
 0x18 N    c10300 50:05:07:64:01:ff:ff:03 20:03:00:05:1e:57:da:5b Conditional

The Local LIRR database has 3 entries

Current LIRR device port number: <XX>
```

When you configure an LIRR entry and it is current, it is marked with -C. If the Management Server marks an entry as current based on order, it is marked with -C. If the Management Server marks an entry as secondary, it is marked with -S.

If the LIRR is configured then the <XX> indicates a valid port number. Otherwise, the line will display the following:

```
Current LIRR device port number is not configured.
```

Node identification data

To display node-identification data, connect to the switch, log in as user, and enter any of the following commands:

- For the local switch: **ficonShow switchrnid**
- For all switches defined in the fabric: **ficonShow switchrnid fabric**
- For all devices registered with the local switch: **ficonShow rnid**
- For all devices registered with all switches defined in the fabric: **ficonShow rnid fabric**

FRU error reporting

FRU failure information is no longer stored on the switch. FRU error information, such as FRU failures and fan and power supply removals and insertions, are stored in error reports as sense data. All FRUs in a chassis have an assigned number that is included in this data. Each CUP instance retains a database of ten FRU error reports. All error reports are sent to host LPARs that have appropriate Current Reporting Paths established with the CUP.

Error reports are added to the database as they occur, then they are removed when sent. If the database fills up, new reports are discarded and not delivered.

Error data

Following are some examples of error data available from the host. The number identifying the failed Brocade FRU (refer to "FRU numbers" on page 73) is derived from a single bit from byte 29 as the high order bit and 4 bits from byte 30 or 31 as the low order bits (refer to the data in bold in the second lines of the following examples). The FRU numbers are decoded for display as the FRU names, which display in the third lines of the following examples.

```
IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 200
      1000A000000000467000100000000000000000000000000000000000000800000
*IRD000E 1065,002032-001 LEVEL=1 FRU(S)=SLOT8

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 286
      1000A000000000467000000000000000000000000000000000000000000880000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=FAN1

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 461
      1000A000000000467000000000000000000000000000000000000000000840000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=PWR4

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 496
      1000A000000000467000000000000000000000000000000000000000000890000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=FAN2

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 502
      1000A000000000467000000000000000000000000000000000000000000810000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=PWR1

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 568
      1000A000000000467000000000000000000000000000000000000000000800000
*IRD000E 1065,002032-001 LEVEL=0 FRU(S)=WWN-CRD

 IOS000I 1065,AB,EQC,**,8200,,,*MASTER*, 662
      1000A000000000467000100000000000000000000000000000000000000A00000
*IRD000E 1065,002032-001 LEVEL=1 FRU(S)=SLOT10

 IOS000I 1061,A8,EQC,**,8200,,,*MASTER*, 697
      1000A000000000467000100000000000000000000000000000000000000700000
*IRD000E 1061,002032-001 LEVEL=1 FRU(S)=SLOT7
```

FRU numbers

Following are the Brocade FRU numbers provided for error reports and associated FRU names that display in error reports. Note that the FRU number does not actually display in the error reports, but its associated FRU name does display.

- 1 = SLOT1
- 2 = SLOT2
- 3 = SLOT3
- 4 = SLOT4
- 5 = SLOT5
- 6 = SLOT6
- 7 = SLOT7
- 8 = SLOT8

- 9 = SLOT9
- 10 = SLOT10
- 11 = SLOT11
- 12 = SLOT12
- 17 = PWR1
- 18 = PWR2
- 19 = PWR3
- 20 = PWR4
- 24 = FAN1
- 25 = FAN2
- 26 = FAN3
- 30 = CHASSIS
- 31 = WWN-CRD

Port swapping

If a port malfunctions, or if you want to connect to different devices without having to re-wire your infrastructure, you can move a port's traffic to another port (*swap ports*) without changing the I/O Configuration Data Set (IOCDS) on the mainframe computer.

ATTENTION
Ports that have been swapped cannot be moved to another logical switch.

NOTE
Ports with area OxFE or OxFF addresses cannot be swapped when FMS mode is enabled.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **portSwapEnable** command to enable the command for port swapping.
3. Enter the **portDisable** command to disable the two ports to be swapped.
4. Enter the **portSwap** command to swap the ports.

   Any port in the switch can be used as the alternate for any other port within the same switch.
5. Re-enable the ports using the **portEnable** command.
6. Enter **portSwapDisable** to disable the command for port swapping.

Example of port swapping

```
switch:admin> portswapenable
switch:admin> portdisable [slot/] portA [slot/]portB
switch:admin> portswap [slot/] portA [slot/]portB
switch:admin> portenable [slot/] portA [slot/]portB
switch:admin> portswapdisable
```

- *slot* is the slot number of the port blade for a system with port blades (optional).
- *portA* is the original port number.
- *portB* is the alternate port number.

You can use the **portSwapShow** command to display information about swapped ports in a switch.

You can use the **portSwap** command to disable the portswap feature. You cannot use the **portSwap** command after this feature is disabled. The enabled state of the portswap feature is persistent across reboots and power cycles. Enabling and disabling the portswap feature does not affect previously executed portswap operations.

See the *Fabric OS Command Reference* for additional details about the **portSwap** command.

Blade swapping

Blade swapping allows you to swap one blade with another of the same type; in this way, you can perform a FRU replacement with minimal traffic disruption. The entire operation is accomplished when the **bladeSwap** command runs on the Fabric OS. The Fabric OS then validates each command before actually implementing the command on the enterprise-class platform. If an error is encountered then blade swap quits without disrupting traffic flowing through the blades. If an unforeseen error does occur during the **bladeSwap** command, an entry will be made into the RASlog and all ports that have been swapped as part of the blade swap operation will be swapped back. On successful completion of the command, the source and destination blades are left in a disabled state allowing you to complete the cable move.

Blade swapping is based on port swapping and has the same restrictions:

- Shared area ports cannot be swapped.
- Ports or blades with area OxFE or OxFF addresses cannot be swapped when FMS mode is enabled.
- Ports that are part of a trunk group cannot be swapped.
- GbE ports cannot be swapped.
- Swapping ports between different logical switches is not supported. The ports on the source and destination blades need to be in the same logical switch.
- Undetermined board types cannot be swapped. For example, a blade swap will fail if the blade type cannot be identified.
- Blade swapping is not supported when swapping to a different model of blade or a different port count. For example, you cannot swap an FC8-32 blade with an FC8-48 port blade.
- Blade swapping is not supported on application blades.

NOTE
This feature is not supported on the FX8-24 DCX Extension blade.

For more information on blade swapping, refer to the *Fabric OS Administrator's Guide*.

Common FICON issues

Any information you need to verify that FICON has been set up correctly can be found in the Chapter 2, “Administering FICON Fabrics” or Chapter 3, “Configuring FICON CUP”.

Symptom *Cascading: No path – Entry Link is “..”*

Probable cause and recommended action

This typically occurs when one or more of the required high integrity features for cascading have not been met. Check the following:

- Review each step in “Configuring switched point-to-point FICON” on page 18 and “Configuring cascaded FICON” on page 21 and validate that all features are configured properly.
- Validate with the data center’s system programmer that CUP is online for each director or switch in the fabric.

Symptom *Path to a device does not come online*

Probable cause and recommended action

Make sure binding or zoning does not prevent the connection. Validate the following with the data center's system programmer:

- Correct switch addresses (not switch IDs) are used in Link statements. Remember that the switch address is the domain ID converted to hex and may have an offset.
- The Switch ID, used in the CHPID statements, was defined with the correct switch address.
- All addressing (LINK statements) uses 2-byte addressing on the channel if 2-byte addressing has been previously used on that channel. This is necessary even when the specified path is not cascaded.

Symptom *Packets are being dropped between two FICON units.*

Probable cause and recommended action

When planning cable needs, the following criteria must be considered:

- Distance considerations
- Fiber Optics Sub Assembly (FOSA) type (SW or LW)
- Cable specifications (SM or MM)
- Patch Panel Connections between FOSA ports (link loss .3-5 dB per)
- Maximum allowable link budget (dB) loss

From a cabling point of view, the most important factor of a Fibre Channel link is the selection of the Fibre Optical Sub Assembly (FOSA) and matching cable type, to support the required distance. Both ends of the optical link must have the matching FOSA (SFP) types.

Symptom *Channel path with 2-byte addressing does not come online*

Probable cause and recommended action

Ask the operator what CHPID he is attempting to bring online. In FICON environments, only the egress ports are defined in the IOCDS. The CHPID number of the channel appears in the node list, but only if the channel path has logged in. If the channel path will not come online, it may not have completed a Fibre Channel fabric login. If this is the case, you will have to rely on customer documentation to determine what switch port the channel is connected to.

Next, ask the operator what type of error message they are getting. An IOS error message is reported when there is an error external to the host; an IEE error message indicates something is wrong internal to the host.

Fabric Not Configured Properly

- Make sure that the insistent domain ID is set and the domain IDs are unique for all switches in the fabric.
- Make sure that the same binding method is used on all switches in the fabric.
- Scroll through the node list and make sure there are no invalid attachments.
- Make sure that the re-routing delay is turned off.

Cabling

Validate that cables are connected where intended.

When using multimode fiber, make sure that all fiber is either all 50u or all 62.5u. A common mistake is to mix 50u and 62.5u fiber cables, which causes errors at patch panels.

Example of a Boxed Channel

In this example, the customer complained that the CHPIDs with 2-byte addressing did not come online. He was instructed to configure the CHPID offline and then try to configure the CHPID back online.

MVS console commands and responses (lines beginning with “IEE” are responses and all other lines are entries.):

```
CF CHP(60),OFFLINE
IEE503I CHP(60),OFFLINE
IEE712I CONFIG PROCESSING COMPLETE
CF CHP(60),ONLINE
IEE754I NOT ALL PATHS BROUGHT ONLINE WITH CHP(60)
IEE502I CHP(60),ONLINE
IEE712I CONFIG PROCESSING COMPLETE
```

The line below displays the status of the CHPID with the “D M =” command. All other lines are responses:

```
D M=CHP(60)
IEE174I 03.29.45 DISPLAY M 021
CHPID 60: TYPE=1D, DESC=FICON INCOMPLETE, ONLINE
DEVICE STATUS FOR CHANNEL PATH 60
    0 1 2 3 4 5 6 7 8 9 A B C D E F
006 . $@ . . . . . . . . . . . . . .
SWITCH DEVICE NUMBER = NONE
ATTACHED ND = NOT KNOWN
PHYSICAL CHANNEL ID = 01F0
********************** SYMBOL EXPLANATIONS ***********************

+ ONLINE @ PATH NOT VALIDATED - OFFLINE . DOES NOT EXIST
```

```
* PHYSICALLY ONLINE $ PATH NOT OPERATIONAL
```

The responses “NOT ALL PATHS BROUGHT ONLINE” after attempting to configure the CHPID online and “FICON INCOMPLETE” after the display command indicate that the channel did not come online. This is determined because the IEE error types are shown and combined with validating that there was no attempt to do a basic FLOGI (no light displayed on the port view (LED) and no Fibre Channel frames were received).

Symptom *The Control Unit Port cannot access the switch.*

Probable cause and recommended action

A 2-byte CHPID (channel path identifier) link is defined using a domain and port ID that must remain consistent. Any change in the physical link, such as a change in a domain or port ID, will prevent storage control unit access.

Use the configure command to verify and set the insistent domain ID (IDID) parameter.

```
FICON:admin> configure

Configure...

  Fabric parameters (yes, y, no, n): [no] y

    Domain: (1..239) [97]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    WAN_TOV: (0..30000) [0]
    MAX_HOPS: (7..19) [7]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
    BB credit: (1..27) [16]

  Insistent Domain ID Mode (yes, y, no, n): [yes] <== this should be set to ‘y’

(output truncated)
```

Symptom *Unable to “vary online” FICON CUP port on the switch*.

Probable cause and recommended action

Use the **haFailover** command on an enterprise class chassis. This the only known fix as there is no known firmware solution.

Symptom *Mainframe RMF utility fails to capture performance data*

Probable cause and recommended action

In Fabric OS v6.0.0, Brocade switches do not fully implement all CUP commands needed to collect all performance data on a switch. Upgrade your switch to Fabric OS v6.1.0, where the performance data is captured.

Troubleshooting FICON

This section provides information gathering and troubleshooting techniques necessary to fix your problem.

General information to gather for all cases

The following information needs to be gathered for all FICON setups:

- The output from the standard support commands (**portLogDump**, **supportSave, supportShow**) the Fabric Manager Event Log, EFCM or Brocade Network Advisor logs.

  By default, the FICON group in the **supportShow** output is disabled. To enable the capture of FICON data in the **supportShow** output, enter the **supportShowCfgEnable ficon** command. After you get confirmation that the configuration has been updated, the following will be collected and appear in the output for the **supportShow** command:

  - ficonCupShow fmsmode
  - ficonCupShow modereg
  - ficonDbg dump rnid
  - ficonDbg log
  - ficonShow lirr
  - ficonShow rlir
  - ficonShow rnid
  - ficonShow switchrnid
  - ficuCmd dump -A
- Type of mainframe involved. Need make, model, and driver levels in use.
- Type of actual storage array installed. Many arrays will emulate a certain type of IBM array and we need to know the exact make, model, and firmware of the array in use.
- Other detailed information for protocol-specific problems:
  - Port data structures, displayed using the **ptDataShow** command.
  - Port registers, displayed using the **ptRegShow** command.
- Read Brocade Release Notes for specific version information regarding the Fabric OS installed.

The following needs to be performed to troubleshoot all FICON setups:

- Perform a **configUpload** to gather configuration files. Provide the IOCDS mainframe file.

  This will define how all mainframe ports are configured.
- Verify that Dynamic Load Sharing (DLS) has been disabled with the **dlsReset** command.

  If DLS is enabled, traffic on existing ISL ports might be affected when one or more new ISLs is added between the same two switches. Specifically, adding the new ISL might result in dropped frames as routes are adjusted to take advantage of the bandwidth provided. By disabling DLS, you ensure that there will be no dropped frames. In a supportshow, search for *route.stickyRoute*s and check for a value of *1* or enter the **dlsShow** command.

- Verify that IOD is enabled using the **iodSet** command to ensure in-order delivery.

  In the output from the **supportShow** or **supportSave**, search for the *route.delayReroute* and check for a value of *1 a*s this indicates that the feature is turned on or enter the **iodShow** command.

Switched point-to-point topology checklist

This checklists lists items you should perform in your FICON environment to ensure proper functionality of the feature:

- Does your Brocade switch or director have Fabric OS v6.1.0 or later release installed?
- Are you using an appropriate management tool such as EFCM v9.6x, DCFM, or Brocade Network Advisor?
- Have you verified that no additional license is required to enable your FICON configuration?
- Have you verified that your switch does not have a special mode setting turned on for FICON?

NOTE
There is no requirement to have a secure fabric in a switched point-to-point topology.

Brocade Advanced features software package (Trunking, Fabric Watch, Extended Fabric) license activation is required.

Cascaded topology checklist

This checklist lists items you should perform in your FICON environment to ensure proper functionality of the feature:

- Verify that your Brocade switch or directory have Fabric OS v6.1.0 or later release installed?
- Verify that you are using an appropriate management tool such as EFCM v9.6x, DCFM, or Brocade Network Advisor?
- Verify that no additional license is required to enable your FICON configuration?
- Verify that your switch does not have a special mode setting turned on for FICON?

  In addition to port-based routing, lossless, and in-order frame delivery (IOD), it is recommended that you enable the dynamic load-sharing feature.
- Verify that if you have a fabric for intermix mode of operations, separate zones for FICON and FCP devices are set?
- Verify the mainframe channel device connectivity rule of maximum one hop is applied to both FCP and FICON devices?
- Verify the Insistent domain ID flag is set to keep the domain ID of a fabric switch persistent?
- Verify the CHPID link path is defined using the 2-byte address format?
- Verify FICON channel connectivity to storage CU port has not exceed one hop?
- Verify that the security policies are enabled? If not, refer to "Configuring cascaded FICON" on page 21.

ATTENTION
The Switch Connection Control (SCC) security policy must be active.

Brocade Advanced features software package (Trunking, Fabric Watch, Extended fabric) license activation is required.

Gathering additional information

In addition to the information you would collect for your support provider mentioned in the *Fabric OS Troubleshooting and Diagnostics Guide*, also gather the following information which is specific to FICON:

- Is this case logged during an initial install or has this environment been working prior to the initial problem?
- What was changed immediately prior to the issue occurring?
- Is the switch properly configured for a FICON environment?

  Also refer to the most recent version of the Fabric OS Release Notes for notes on FICON setup and configuration.
- Is this a switched point-to-point or cascaded environment?
- Is the FICON group enabled for supportshow?

  Check at the top of the supportshow. If not, use **supportShowCfgEnable ficon** and re-run the test that was failing.

NOTE
If this setting is not set to port-based routing on the Brocade 4100, 4900, or 5000 switches and the Brocade 48000 director in a FICON fabric, you will experience excessive interface control checks (IFCCs) on the mainframe whenever a blade or CP is hot-plugged or unplugged.

Troubleshooting FICON CUP

In addition to the information you would collect for your support provider mentioned "Troubleshooting FICON" on page 79, also gather the following information which is specific to FICON CUP:

- Capture all data from the "General information to gather for all cases" on page 79.
- Verify the FICON CUP license is installed.
- Check the state of the CUP port by running the **ficonCupShow fmsmode** command. If it is disabled, type the **ficonCupSet fmsmode enable** command to enable it. If this is on a directory, enter the **haFailover** command to ensure both CPs are set correctly.
- Verify that the director has a Fabric OS v6.1.0 or later.
- Ensure no device is plugged into port 254 on the Brocade 48000 or Brocade DCX enterprise-class platform.
- Verify with the systems programmer that the CUP ports are defined properly.

  FICON ports are defined as part of the sysgen process. The z/OS systems programmer can verify if the CUP ports are defined properly.

- Verify the ports 254 and 255 display the *Disabled (FMS Mode)* by entering the **switchShow** command. If not, enter the **portDisable** command on the appropriate models for the related ports:
  - On a Brocade 48000 disable 10/30 and 10/31.
  - On a Brocade DCX Backbone disable 12/30 and 12/31.

Troubleshooting NPIV

You should capture all pertinent data from the "General information to gather for all cases" on page 79 and "Gathering additional information" on page 81.

NPIV licenses must be installed on v5.0.x. There is no license requirement for Fabric OS v5.1.0 and later.

Appendix

Configuration Information Record

A

You can use the following worksheet (Table 6) for recording FICON configuration information.

TABLE 6 FICON configuration worksheet

FICON® Switch Configuration Worksheet									
FICON® Switch Manufacturer:_____Type: _____ Model: _____ S/N: _____									
HCD Defined Switch ID_____(Switch ID) FICON® Switch Domain ID_____(Switch @)					Cascaded Directors No _____Yes _____ Corresponding Cascaded Switch Domain ID _____ Fabric Name _____				
FICON® Switch F_Ports					Attached N_Ports / E_Ports (CU, CPC, or ISL)				
Slot Number	Port Number	Port Address	Laser Type: LX / SX	Port Name	Node Type CU / CHNL	Machine Type	Model	Serial Number	ISL CU I/F CPC CHPID

Appendix

EBCDIC Code Page

B

Extended Binary Coded Decimal Interchange Code (EBCDIC) is an 8-bit character encoding (code page) used on IBM mainframe operating systems such as z/OS and S/390. Code page 37 is an EBCDIC code page with full Latin-1-charset.

EBCDIC Code Page 00037

	–0	–1	–2	–3	–4	–5	–6	–7	–8	–9	–A	–B	–C	–D	–E	–F
0–	NUL 0000 *0*	SOH 0001 *1*	STX 0002 *2*	ETX 0003 *3*	SEL *4*	HT 0009 *5*	RNL *6*	DEL 007F *7*	GE *8*	SPS *9*	RPT *10*	VT 000B *11*	FF 000C *12*	CR 000D *13*	SO 000E *14*	SI 000F *15*
1–	DLE 0010 *16*	DC1 0011 *17*	DC2 0012 *18*	DC3 0013 *19*	RES ENP *20*	NL 0085 *21*	BS 0008 *22*	POC *23*	CAN 0018 *24*	EM 0019 *25*	UBS *26*	CU1 *27*	IFS 001C *28*	IGS 001D *29*	IRS 001E *30*	IUS ITB 001F *31*
2–	DS *32*	SOS *33*	FS *34*	WUS *35*	BYP INP *36*	LF 000A *37*	ETB 0017 *38*	ESC 001B *39*	SA *40*	SFE *41*	SM SW *42*	CSP *43*	MFA *44*	ENQ 0005 *45*	ACK 0006 *46*	BEL 0007 *47*
3–	*48*	*49*	SYN 0016 *50*	IR *51*	PP *52*	TRN *53*	NBS *54*	EOT 0004 *55*	SBS *56*	IT *57*	RFF *58*	CU3 *59*	DC4 0014 *60*	NAK 0015 *61*	*62*	SUB 001A *63*
4–	SP 0020 *64*	RSP 00A0 *65*	â 00E2 *66*	ä 00E4 *67*	à 00E0 *68*	á 00E1 *69*	ã 00E3 *70*	å 00E5 *71*	ç 00E7 *72*	ñ 00F1 *73*	¢ 00A2 *74*	. 002E *75*	< 003C *76*	(0028 *77*	+ 002B *78*	| 007C *79*
5–	& 0026 *80*	é 00E9 *81*	ê 00EA *82*	ë 00EB *83*	è 00E8 *84*	í 00ED *85*	î 00EE *86*	ï 00EF *87*	ì 00EC *88*	ß 00DF *89*	! 0021 *90*	$ 0024 *91*	* 002A *92*	) 0029 *93*	; 003B *94*	¬ 00AC *95*
6–	- 002D *96*	/ 002F *97*	Â 00C2 *98*	Ä 00C4 *99*	À 00C0 *100*	Á 00C1 *101*	Ã 00C3 *102*	Å 00C5 *103*	Ç 00C7 *104*	Ñ 00D1 *105*	¦ 00A6 *106*	, 002C *107*	% 0025 *108*	_ 005F *109*	> 003E *110*	? 003F *111*
7–	ø 00F8 *112*	É 00C9 *113*	Ê 00CA *114*	Ë 00CB *115*	È 00C8 *116*	Í 00CD *117*	Î 00CE *118*	Ï 00CF *119*	Ì 00CC *120*	` 0060 *121*	: 003A *122*	# 0023 *123*	@ 0040 *124*	' 0027 *125*	= 003D *126*	" 0022 *127*
8–	Ø 00D8 *128*	a 0061 *129*	b 0062 *130*	c 0063 *131*	d 0064 *132*	e 0065 *133*	f 0066 *134*	g 0067 *135*	h 0068 *136*	i 0069 *137*	« 00AB *138*	» 00BB *139*	ð 00F0 *140*	ý 00FD *141*	þ 00FE *142*	± 00B1 *143*
9–	° 00B0 *144*	j 006A *145*	k 006B *146*	l 006C *147*	m 006D *148*	n 006E *149*	o 006F *150*	p 0070 *151*	q 0071 *152*	r 0072 *153*	ª 00AA *154*	º 00BA *155*	æ 00E6 *156*	, 00B8 *157*	Æ 00C6 *158*	¤ 00A4 *159*
A–	µ 00B5 *160*	~ 007E *161*	s 0073 *162*	t 0074 *163*	u 0075 *164*	v 0076 *165*	w 0077 *166*	x 0078 *167*	y 0079 *168*	z 007A *169*	¡ 00A1 *170*	¿ 00BF *171*	Ð 00D0 *172*	Ý 00DD *173*	Þ 00DE *174*	® 00AE *175*
B–	^ 005E *176*	£ 00A3 *177*	¥ 00A5 *178*	· 00B7 *179*	© 00A9 *180*	§ 00A7 *181*	¶ 00B6 *182*	¼ 00BC *183*	½ 00BD *184*	¾ 00BE *185*	[005B *186*	] 005D *187*	¯ 00AF *188*	¨ 00A8 *189*	´ 00B4 *190*	× 00D7 *191*
C–	{ 007B *192*	A 0041 *193*	B 0042 *194*	C 0043 *195*	D 0044 *196*	E 0045 *197*	F 0046 *198*	G 0047 *199*	H 0048 *200*	I 0049 *201*	SHY 00AD *202*	Ô 00F4 *203*	ö 00F6 *204*	ò 00F2 *205*	ó 00F3 *206*	õ 00F5 *207*
D–	} 007D *208*	J 004A *209*	K 004B *210*	L 004C *211*	M 004D *212*	N 004E *213*	O 004F *214*	P 0050 *215*	Q 0051 *216*	R 0052 *217*	¹ 00B9 *218*	û 00FB *219*	ü 00FC *220*	ù 00F9 *221*	ú 00FA *222*	ÿ 00FF *223*
E–	\ 005C *224*	÷ 00F7 *225*	S 0053 *226*	T 0054 *227*	U 0055 *228*	V 0056 *229*	W 0057 *230*	X 0058 *231*	Y 0059 *232*	Z 005A *233*	² 00B2 *234*	Ô 00D4 *235*	Ö 00D6 *236*	Ò 00D2 *237*	Ó 00D3 *238*	Õ 00D5 *239*
F–	0 0030 *240*	1 0031 *241*	2 0032 *242*	3 0033 *243*	4 0034 *244*	5 0035 *245*	6 0036 *246*	7 0037 *247*	8 0038 *248*	9 0039 *249*	³ 00B3 *250*	Û 00DB *251*	Ü 00DC *252*	Ù 00D9 *253*	Ú 00DA *254*	EO *255*

B EBCDIC Code Page

Index

A

address mode
    changing, *24*
addressing modes, *22*

B

binding, *11*

C

cascade mode topology checklist, *80*
cascaded configuration, *7*
clearing the management database, *24*
clearing the RLIR database, *13*
configuration file
    fmsmode, *63*
    restoring in a FICON environment, *62*
configuring switch, single, *17*
Control Unit Port cannot access the switch, *78*
creating the SCC policy, *16*
CUP, *13*, *27*

D

disabling IDID mode, *13*
disabling the management server mode, *13*
displaying information, *71*
DLS, *79*
domain ID, insistent, *2*
Dynamic Load Sharing, *79*

E

enabling IDID mode, *13*
extension
    configuration requirements, *48*
    DASD application, *44*
    determinate path, *48*
    emulation, *50*
    emulation concepts, *43*
    emulation configuration values, *51*
    emulation, monitoring, *53*
    FCIP tunnels, *48*
    performance, *53*
    Traffic Isolation zoning, *49*

F

fabric binding, *11*
Fibre Channel Association, *xi*
FICON CUP, *13*, *27*
FMS mode
    disabling, *35*
    displaying, *35*
    enabling, *35*
    OxFE and OxFF addresses, *36*
    setting up FICON CUP, *35*
    upgrade considerations, *36*
FRU failures, *72*

G

gathering additional information, *79*, *81*
Global Mirror emulation, *44*

I

IBM z/OS Global Mirror emulation, *44*
identifying ports from the tag field, *71*
IDID, *2*
insistent domain ID, *2*
intermix mode, *1*
invalid attachment/isolated state, *15*

L

link incidents, *14*
link incidents, displaying, *14, 71*
LIRR, *14*

M

mainframe RMF utility, *78*
meeting QSA requirements, *15*

N

node identification data, *72*
node identification, display, *14*

O

Optica Prizm support, *47*
OxFE and OxFF addresses for FMS mode, *36*

P

packets being dropped, *76*
persistently enabling/disabling ports, *40*
port and switch naming standards, *30*
port swapping, *74*

Q

QSA requirements, *15*

R

recording configuration information, *38*
registered listeners, *14, 72*
RLIR
    clearing the database, *13*
    link incidents, displaying, *14*
RNID node identification, *14*

S

SCC policy, *16*
security policy, create, *21*
security-related commands, *16*
single-switch configuration, *17*
switch preparation, *17*
switched point-to-point configuration, *6*

T

tag field, interpreting, *71*
Tape Pipelining, *50*
Teradata emulation, *47*
Teradata statistics, *55*
troubleshooting NPIV, *82*

U

unable to 'vary online', *78*

X

XRC, *44*

Z

zoning and PDCM considerations, *13*